PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-205310
(43)Date of publication of application : 30.07.1999

(51)Int.CI. H04L 9/36
H04L 9/14
H04L 12/40

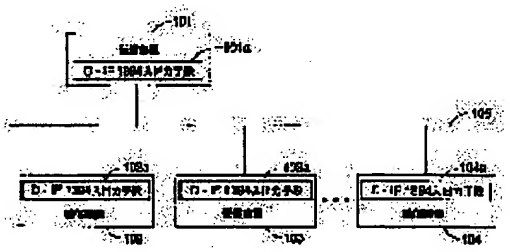
(21)Application number : 10-307358
(22)Date of filing : 28.10.1998

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : IIZUKA HIROYUKI
YAMADA MASAZUMI
TAKECHI HIDEAKI
MATSUZAKI NATSUME

(30)Priority
Priority number : 09297614 Priority date : 29.10.1997 Priority country : JP

(54) DATA TRANSMISSION METHOD, DATA RECEPTION METHOD, DATA TRANSMISSION SYSTEM AND PROGRAM RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To further surely protect transmission data by deciding the kind of ciphering to be applied corresponding to the management information of data, enciphering the data and transmitting them together with management information.
SOLUTION: The mode decision means of a transmitter 101 decides the group of a cryptographic key to be used corresponding to the contents of the copy management information of video data or the like to be transmitted and outputs it to a key generation means as cipher mode information. The key generation means generates a key to be used for enciphering within the decided group (A or B) of the key, based on it. When information is sent from a mode detection means, the key obtaining means of a receiver 102 sends the transfer request of key information for starting the obtaining of the key to a D-IF1394 input/output means 102a. The key obtaining means sends the key information transferred from the side of the transmitter 101 to a key preservation means and it is temporarily preserved there and outputted to an enciphering means. The deciphering means deciphers actual data by utilizing the key information from the key preservation means and key change information from a packet decoding means.



LEGAL STATUS
[Date of request for examination] 16.08.2001

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The data transmitting approach characterized by determining the class of encryption applied to transmission of said data according to the management information of the data used as the candidate for transmitting, enciphering said data based on the class of the determined encryption, and transmitting said enciphered data and said data control information.
[Claim 2] The data receiving approach characterized by receiving the transmit data transmitted by the data transmitting approach according to claim 1, detecting said data control information from the received data, and requiring the decryption information corresponding to delivery and its transmitted data control information for said detected data control information from the transmitting origin of said transmit data.
[Claim 3] The data transmitting approach according to claim 1 characterized by transmitting said decryption information corresponding to said data control information to said demand origin when there is a demand of said decryption information by the data receiving approach according to claim 2.
[Claim 4] The data receiving approach according to claim 2 characterized by decrypting said received data and determining the method of processing of said decrypted received data according to said detected data control information based on said decryption information transmitted by the data transmitting approach according to claim 3.
[Claim 5] The data transmitting approach according to claim 1 or 3 characterized by transmitting the preliminary announcement information which announces performing said updating beforehand before updating the class of said encryption with time amount, enciphering the data used as said candidate for transmitting according to the class of said updated encryption and transmitting said enciphered data, even if it is the case that said data control information is the same.
[Claim 6] The data transmitting approach according to claim 1 or 3 characterized by to transmit the both sides of the decryption information which should be used at the time, and the decryption information on the schedule used at the next time when the class of said encryption is updated with time amount, it transmits the information which shows that said updating was performed and there is a demand of the decryption information corresponding to said data-control information, even if it is the case that said data-control information is the same.
[Claim 7] The data transmitting approach according to claim 5 or 6 characterized by the class of the updated encryption of said not overlapping the class of encryption of others [above / which was determined according to said data control information] when updating the class of said encryption with time amount.
[Claim 8] The data receiving approach according to claim 2 or 4 characterized by requiring said decryption information from the transmitting origin of said transmit data according to the preliminary announcement information when said preliminary announcement information transmitted by the data transmitting approach according to claim 5 is received.
[Claim 9] The data receiving approach according to claim 2 or 4 characterized by requiring said decryption information to the transmitting origin of said information based on the received information when the information which shows that said updating transmitted by the data transmitting approach according to claim 6 was performed is received.
[Claim 10] The data receiving approach according to claim 2 or 8 characterized by being sending said detected data control information as it is as sending said data control information, or performing

predetermined conversion and sending said detected data control information.
[Claim 11] The data transmitting approach according to claim 1 or 3 characterized by being changing the key used for encryption according to said data control information as determining the class of encryption applied to transmission of said data according to said data control information.
[Claim 12] The data transmitting approach according to claim 1 or 3 characterized by being changing the algorithm used for encryption according to said data control information as determining the class of encryption applied to transmission of said data according to said data control information.
[Claim 13] a 1-time copy is possible for said data control information in whether said data are copy freedom -- or the data transmitting approach according to claim 1, 3, 5, or 6 characterized by being copy management information including the information which shows whether it is the ban on a copy.
[Claim 14] With the information which shows that it is the ban on a copy from origin to the information which shows that it is the ban on said copy, from the first, once, although the copy was possible It is the data transmitting approach according to claim 13 which two kinds of information on the information which shows the ban on the further copy which means that the subsequent copy was forbidden is included since the one copy was performed, and is characterized by the classes of said encryption differing according to these two kinds of information.
[Claim 15] The data control information transmitted by the data transmitting approach according to claim 13 When it is shown once that a copy is possible and the data which have the information which shows once [said] that a copy is possible as data control information are recorded on a predetermined record medium, The data receiving approach according to claim 8 or 9 characterized by performing said record with the data control information which changes into the contents which show the ban on a copy since said 1-time copy of the data control information is possible, and shows the ban on the copy.
[Claim 16] The data control information transmitted by the data transmitting approach according to claim 14 When it is shown once that a copy is possible and the data which have the information which shows once [said] that a copy is possible as data control information are recorded on a predetermined record medium, The data receiving approach according to claim 8 or 9 characterized by performing said record with the data control information which changes into the contents which show the ban on said further copy since said 1-time copy of the data control information is possible, and shows the ban on the further copy.
[Claim 17] A mode decision means to determine the class of encryption applied to transmission of said data according to the management information of the data used as the candidate for transmitting, An encryption means to encipher said data based on the class of the determined encryption, A data transmitting means to transmit said enciphered data and said data control information, A data receiving means to receive the transmit data transmitted by said data transmitting means, A data control information detection means to detect said data control information from the received data, A decryption information-requirements means to require the decryption information corresponding to delivery and its transmitted data control information for said detected data control information from the transmitting origin of said transmit data, A decryption information transmitting means to transmit said decryption information corresponding to said data control information to said demand origin when there is a demand of said decryption information, The data transmission system characterized by having a decryption means to decrypt said received data, and an art decision means to determine the method of processing of said decrypted received data according to said detected data control information, based on said said transmitted decryption information.
[Claim 18] The data transmission system according to claim 17 characterized by being sending said detected data control information as it is as sending said data control information, or performing predetermined conversion and sending said detected data control information.
[Claim 19] The data transmission system according to claim 17 characterized by being changing the key used for encryption according to said data control information as determining the class of encryption applied to transmission of said data according to said data control information.
[Claim 20] The data transmission system according to claim 17 characterized by being changing the algorithm used for encryption according to said data control information as determining the class of encryption applied to transmission of said data according to said data control information.
[Claim 21] A renewal means of an encryption class to update the class of said encryption with time amount even if it is the case that said data control information is the same, It has a preliminary announcement information generation means to generate the preliminary announcement information for announcing

performing said updating beforehand. The data with which said encryption means serves as said candidate for transmitting When [said] enciphering, The data transmission system according to claim 17 characterized by being transmitted before transmitting the data with which it enciphered according to the class of said updated encryption, and said generated preliminary announcement information was enciphered by the class of said updated encryption.

[Claim 22] A renewal means of an encryption class to update the class of said encryption with time amount even if it is the case that said data control information is the same, It has an updating execution information generation means to generate the update information for notifying having performed said updating. The data with which said encryption means serves as said candidate for transmitting When [said] enciphering, The data transmission system according to claim 17 characterized by transmitting said update information in case transmission of the data which enciphered according to the class of said updated encryption, and were enciphered by the class of said updated encryption is started.

[Claim 23] Said decryption information-requirements means is the data transmission system of claim 21 characterized by requiring said decryption information from the transmitting origin of said transmit data according to said received preliminary announcement information.

[Claim 24] Said decryption information-requirements means is a data transmission system according to claim 22 characterized by requiring said decryption information to the transmitting origin of said transmit data according to change of said received update information.

[Claim 25] Any of claims 21-24 characterized by the class of the updated encryption of said not overlapping the class of encryption of others [above / which was determined according to said data control information] when updating the class of said encryption with time amount, or the data transmission system of one publication.

[Claim 26] a 1-time copy is possible for said data control information in whether said data are copy freedom -- or any of claims 17-25 characterized by being copy management information including the information which shows whether it is the ban on a copy or the data transmission system of one publication.

[Claim 27] It is the data transmission system according to claim 26 two kinds of the information on the information shown in the ban on the information which shows from origin that it is the ban on a copy, and the further copy which mean that a subsequent copy was forbidden since the one copy was performed once from the first, although the copy was possible is included in the information which shows that it is the ban on said copy, and carry out that the class of said encryption differs according to these two kinds of information as the description.

[Claim 28] When the data control information transmitted by said data transmitting means shows once that a copy is possible, When the data which have the information which shows once [said] that a copy is possible as data control information are recorded on a predetermined record medium, The data transmission system according to claim 26 characterized by changing the data control information into the contents which show the ban on a copy once [said] since a copy is possible, and performing said record with the data control information which shows the ban on the copy.

[Claim 29] When the data control information transmitted by said data transmitting means shows once that a copy is possible, When the data which have the information which shows once [said] that a copy is possible as data control information are recorded on a predetermined record medium, The data transmission system according to claim 27 characterized by changing the data control information into the contents which show the ban on said further copy once [said] since a copy is possible, and performing said record with the data control information which shows the ban on the further copy.

[Claim 30] The program documentation medium characterized by recording the program for making a computer perform any of claims 1-16, or all or a part of steps of each steps of one publication.

[Claim 31] The program documentation medium characterized by recording the program for making any one claim of claims 17-29 perform the function of all or a part of means of each means of a publication to a computer.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the data transmitting approach which transmits and receives digital data, the data receiving approach, a data transmission system, and a program documentation medium.
[0002]
[Description of the Prior Art] There is the data transfer approach which used IEEE1394 specification (IEEE: THE INSTITUTE OFELECTRICAL AND ELECTRINIC ENGINEERS, INC) in the conventional data transfer method. (Bibliography: IEEE1394 High Performance Serial Bus) The data transfer in IEEE1394 specification has the eye SOKURONOSU communication link suitable for synchronous data transfers, such as a video signal and a sound signal, and the ray synchronous communication link suitable for a transfer of asynchronous datas, such as a control signal, and both communication links can be intermingled on an IEEE1394 bus.
[0003] An eye SOKURONOSU communication link is the so-called broadcast type of communication link, and the eye SOKURONO spa blanket which a certain equipment on an IEEE1394 bus outputs can receive all the equipments on this bus.
[0004] On the other hand, a ray synchronous communication link has both the communication link of 1 to 1, and a broadcast mold communication link. And the identifier showing the equipment which should receive the packet is contained in the ray synchronous packet which a certain equipment on a bus outputs, when the identifier expresses specific equipment, the equipment specified by the identifier receives the ray synchronous packet concerned, and when an identifier expresses broadcasting, all the equipments on this bus receive the ray synchronous packet concerned.
[0005] Moreover, using IEEE1394 specification, a digital sound signal, a digital video signal, etc. are transmitted, or IEC61883 specification (AV protocol is called hereafter) is examined in IEC (IEC:InternationalElectrotechnical Commission Electrotechnical International Commission) as specification for performing connection management of a data transmission path between the devices connected on the IEEE1394 bus. In AV protocol, image voice data is arranged and transmitted in an eye SOKURONO spa blanket. Moreover, an eye SOKURONO spa blanket contains a CIP header (CIP: Common Isochronous Packet). In the CIP header, information, such as the device number of the identification information which shows the class of image voice data, and the sending set which has transmitted the eye SOKURONO spa blanket, is included.
[0006] In the data transmission system using such a conventional data transfer method, the data transmission system which can restrict the copy of data used as the candidate for a transfer using data protection information from a viewpoint of the protection of copyrights of the data used as the candidate for transmitting is proposed. thus, the video data which digitized the image as digital data which needs the structure of a copy limit, for example and the audio data which digitized voice -- or there is digital data constituted by doubling both.
[0007] Below, the configuration is described about such a conventional data transmission system, referring to drawing 6 .
[0008] That is, drawing 6 is drawing showing a format of the eye SOKURONO spa blanket used with the conventional data transmission system.

[0009] The eye SOKURONO spa blanket 101 consists of the eye SOKURONOSU packet header 900, a header CRC 901, an eye SOKURONOSU payload 902, and data CRC 903 as shown in this drawing.
[0010] The Sy field 910 for storing data protection information is included in the eye SOKURONOSU packet header 900. When the value stored in 2 bits of high orders of the Sy field 910 is 00, it is shown that the data (live data 905 mentioned later) used as the candidate for transmitting are data which can copy freely. Moreover, when it is 11 further about the ability of the data to copy once when it is 10, the data shows that it is the ban on a copy.
[0011] Moreover, the 2-bit tag 907 is contained in the eye SOKURONOSU packet header 900. A tag 907 shows that it is the eye SOKURONO spa blanket with which the eye SOKURONO spa blanket was based on AV protocol, when the value is 01. When the value of a tag 907 is 01, namely, when the eye SOKURONO spa blanket is an eye SOKURONO spa blanket of AV protocol conformity, the CIP header 904 is contained at the head of the eye SOKURONOSU payload 902.
[0012] In the CIP header 904, the source ID 906 which is the identifier of the output unit which is outputting the eye SOKURONO spa blanket concerned is contained. Moreover, FMT908 and FDF909 showing what kind of data the live data 905 contained in the eye SOKURONOSU payload 902 are are contained in the CIP header 904.
[0013] In the case of 00 which means a copy free-lancer, encryption is not carried out although it is data enciphered when the data protection information which these live data 905 mentioned above was 10 or 11 although the data set as the transmitting object of an image or voice were contained in live data 905. Moreover, data protection information is included also in live data 905, and generally, in the case of CD, it is referred to as SCMS, and, in the case of DV, is referred to as CGMS etc.
[0014] In such a configuration, actuation is explained below. Namely, in case a transmitter transmits digital data, it stores in the Sy field 910 of the eye SOKURONOSU packet header 900 the data protection information which shows the conditions of whether to copy, and transmits it with live data 905. A receiver side detects data protection information out of the Sy field 910 of the received data, and changes actuation of the device when recording digital data based on the result of having interpreted the contents of data protection information. Moreover, since live data are enciphered except for the case where it is a copy free-lancer's data, a receiver side requires a transfer of decryption information required in order to decrypt it of a transmitter side. A transmitter sends decryption information to the demand origin in response to the demand. A receiver decrypts the live data 905 which received using the decryption information sent from the transmitter. Thus, the decrypted live data 905 are displayed on a display. On the other hand, about record actuation of the decrypted live data, it changes suitably based on the contents of data protection information.
[0015] That is, if a receiver is VTR, when the detected data protection information means "one copy is possible", the decrypted data are recorded on the video tape built in VTR. Moreover, record actuation will not be performed even if the image transcription carbon button was pushed, when "the ban on a copy" was meant.
[0016]
[The technical problem which invention makes solution ******] However, in such a conventional data transmission system, when the data protection information stored in the Sy field 910 all over the transmission line between a transmitter side and a receiver side by those who are going to perform a malfeasance was altered, it had the technical problem that the decrypted data will be copied unjustly.
[0017] That is, for example, in the phase transmitted from the transmitter, the value of the data protection information stored in the Sy field 910 of the eye SOKURONOSU packet header 900 is 11, and when "the ban on a copy" is meant, a malfeasance person presupposes that the value of the data protection information was altered to 10 which means "one copy is possible" in a transmission line. Hereafter, it attaches in this case and explains still more concretely.
[0018] That is, VTR by the side of a receiver looks at the data protection information stored in the Sy field 910 in this case, and it detects that that value is 10. In this case, live data 905 send the Request to Send of the decryption information for decrypting it, since it is enciphered like mentioned above to a transmitter. The transmitter which received this demand sends decryption information to the receiver of a requiring agency. A receiver side displays the decrypted live data on a display etc., after decrypting live data 905

using the sent decryption information. Since it had detected that the value of the data protection information stored in the Sy field 910 was 10 on the other hand as VTR was mentioned above, although the live data 905 which received were originally data of the ban on a copy, it judged that one copy was possible and had the technical problem that the live data by which the decryption was carried out [above-mentioned] will be recorded on videotape on a video tape.

[0019] This invention aims to let protection of transmission data offer the data transmitting approach which can be performed much more certainly compared with the former, the data receiving approach, a data transmission system, and a program documentation medium in consideration of such a technical problem of the above-mentioned conventional data transmission system.

[0020]

[Means for Solving the Problem] The 1st this invention (it corresponds to invention according to claim 1) is the data transmitting approach of determining the class of encryption applied to transmission of said data according to the management information of the data used as the candidate for transmitting, enciphering said data based on the class of the determined encryption, and transmitting said enciphered data and said data control information.

[0021] Moreover, the 2nd this invention (it corresponds to invention according to claim 2) is the data receiving approach of receiving the transmit data transmitted by the data transmitting approach of the 1st this invention of the above, detecting said data control information from the received data, and requiring the decryption information corresponding to delivery and its transmitted data control information for said detected data control information from the transmitting origin of said transmit data.

[0022] Moreover, the 3rd this invention (it corresponds to invention according to claim 3) is the data transmitting approach of the 1st this invention of the above of transmitting said decryption information corresponding to said data control information to said demand origin, when there is a demand of said decryption information by the data receiving approach of the 2nd this invention of the above.

[0023] Moreover, the 4th this invention (it corresponds to invention according to claim 4) is the data receiving approach of the 2nd this invention of the above of decrypting said received data and determining the method of processing of said decrypted received data according to said detected data control information based on said decryption information transmitted by the data transmitting approach of the 3rd this invention of the above.

[0024] Moreover, the 17th this invention (it corresponds to invention according to claim 17) A mode decision means to determine the class of encryption applied to transmission of said data according to the management information of the data used as the candidate for transmitting, An encryption means to encipher said data based on the class of the determined encryption, A data transmitting means to transmit said enciphered data and said data control information, A data receiving means to receive the transmit data transmitted by said data transmitting means, A data control information detection means to detect said data control information from the received data, A decryption information-requirements means to require the decryption information corresponding to delivery and its transmitted data control information for said detected data control information from the transmitting origin of said transmit data, A decryption information transmitting means to transmit said decryption information corresponding to said data control information to said demand origin when there is a demand of said decryption information, It is the data transmission system equipped with a decryption means to decrypt said received data, and an art decision means to determine the method of processing of said decrypted received data according to said detected data control information, based on said said transmitted decryption information.

[0025] Moreover, the 21st this invention (it corresponds to invention according to claim 21) A renewal means of an encryption class to update the class of said encryption with time amount even if it is the case that the above-mentioned data control information is the same, It has a preliminary announcement information generation means to generate the preliminary announcement information for announcing performing said updating beforehand. The data with which said encryption means serves as said candidate for transmitting When [said] enciphering, It is the data transmission system of the 17th this invention of the above transmitted before transmitting the data with which it enciphered according to the class of said updated encryption, and said generated preliminary announcement information was enciphered by the class of said updated encryption.

[0026] Moreover, the 22nd this invention (it corresponds to invention according to claim 22) A renewal means of an encryption class to update the class of said encryption with time amount even if it is the case that the above-mentioned data control information is the same, It has an updating execution information generation means to generate the update information for notifying having performed said updating. The data with which said encryption means serves as said candidate for transmitting When [said] enciphering, In case transmission of the data which enciphered according to the class of said updated encryption, and were enciphered by the class of said updated encryption is started, it is the data transmission system of the 17th this invention of the above with which said update information is transmitted.
[0027] By the above configuration, protection of transmission data can perform this invention much more certainly compared with the former.
[0028]
[Embodiment of the Invention] Hereafter, the gestalt of 1 operation of the data transmission system of this invention is explained, referring to a drawing.
[0029] Drawing 1 is the outline block diagram having shown the whole data transmission system of the gestalt of this operation, and drawing 2 and 3 are the block diagrams about the sending set which constitutes the data transmission system, and a receiving set.
[0030] Hereafter, the configuration of the gestalt of this operation is described using this drawing.
[0031] As shown in drawing 1 , as for the data transmission system of the gestalt of this operation, two or more receiving sets 102-104 are connected with the sending set 101 by the IEEE1394 bus 105. Connection between each equipment 101-104 and the IEEE1394 bus 105 is made through the D-IF1394 I/O means (101a-104a).
[0032] Moreover, the data transfer between a sending set 101 and two or more receiving sets 102-104 is the same as that of the thing explaining the conventional data transmission system. That is, the eye SOKURONOSU communication link suitable for synchronous data transfers, such as a video signal and a sound signal, and the ray synchronous communication link suitable for a transfer of asynchronous datas, such as a control signal, have composition which can be intermingled on the IEEE1394 bus 105.
[0033] Next, the internal configuration of the sending set 101 of the gestalt of this operation is described using drawing 2 .
[0034] That is, as shown in drawing 2 , the data output means 201 is a means to output the image data of the predetermined length who is going to transmit on 1394 buses 105 etc. to the mode decision means 202 and the encryption means 205. The mode decision means 202 is a means to determine of which group a key is used as a key of encryption according to the contents of copy management information, such as image data which it is going to transmit, and to output to the key generating means 203 by making the determined contents into code mode information. Correspondence with copy management information and encryption mode is mentioned further later. With the gestalt of this operation, copy management information presupposes that they are a copy free-lancer, the one copy possibility of, and the information that shows the level of protection of three kinds of copyrights of the ban on a copy. The copy management information of the gestalt of this operation corresponds to the data control information on this invention. Moreover, the key generating means 203 is a means to generate key 203a used for encryption into the group (groups A and B) of the determined key according to the code mode information from the mode decision means 202. Generating of this key is performed one by one in time according to change information 207a from the change timing decision means 207, and all the keys generated differ.
[0035] Here, correspondence with copy management information and encryption mode is further described as mentioned above.
[0036] namely, -- the gestalt of this operation -- the three above-mentioned kinds of copy management information -- corresponding -- a copy free-lancer -- if -- it shall not encipher, if one copy is possible, a cryptographic key shall be determined out of Group A, and in the ban on a copy, a cryptographic key shall be determined out of Group B If it puts in another way, encryption mode information will be information which identifies the group of a cryptographic key. In addition, Group A and Group B presuppose that it does not have a common key.
[0037] Moreover, the key preservation means 204 saves temporarily key 203a generated by the key generating means 203, and is a means to output saved key 203a to the encryption means 205. The

encryption means 205 is a means to encipher using key 203a to which image data 201a outputted from the data output means 201 has been sent from the key preservation means 204, and to output encryption data 205a to the PAKKETTO generation means 209. The key distribution means 206 is a means which changes the purport which distributed key 203a based on authentication of a requiring agency, and its authentication result by asynchronous communication, and distribution of key 203a completed according to the demand from a receiving set, and is sent to the timing decision means 207. A change timing decision means 207 is a means determine the change stage of a key for updating the key used for encryption with time amount into the group of the key which was mentioned above, and which was determined by the mode decision means 202 like, and is a means send change information 207a which shows the change stage to the key generating means 203 and the modification information generating means 208. The modification information generating means 208 acquires the information from the key distribution means 206 and the change timing decision means 207, and is the Inn-transition. It is a means to create mode information and it is a means to output alternatively the copy management information (code mode and correspondence) and the Inn-transition mode information which are sent from the mode decision means 202 to the packet generation means 209.

[0038] It is the information for announcing beforehand in advance the timing from which a key is changed into the same code mode as the Inn-transition mode information here.

[0039] Moreover, with the gestalt of this operation, each of code mode information and Inn-transition mode information is data 208a which is stored in the Sy field 910 in the eye SOKURONOSU packet header 900 stated by drawing 6 , and consists of 2 bits.

[0040] Moreover, the correspondence with the pattern of this 2 bit-data 208a, and copy management information (code mode information and correspondence) and the Inn-transition mode information is as follows.

[0041] That is, in a copy free-lancer, if 00 and one copy are possible for copy management information, by 10 and the ban on a copy, it shall set to 11 and shall apply 01 to the Inn-transition mode.

[0042] The packet generation means 209 is a means to obtain encryption data 205a (for it to correspond to the live data 905 of drawing 6), and 2 bit-data 208a stored in Sy field, to generate data packet 209a transmitted to up to a data bus 105 by synchronous transmission, and to output it to D-IF1394 I/O means 101a. In addition, with the configuration of this operation, the configuration of a data packet is fundamentally [as the configuration stated at drawing 6] the same.

[0043] Moreover, D-IF1394 I/O means 101a performs I/O of an eye SOKURONO spa blanket and a ray synchronous packet between 1394 buses 105 and a sending set 101. That is, while outputting data packet 209a (eye SOKURONO spa blanket) which the packet generation means 209 outputs, and key information 203a (ray synchronous packet) which the key distribution means 206 outputs on 1394 buses 105, it is a means to output the ray synchronous packet which received from 1394 buses 105 to the key distribution means 206.

[0044] Next, the internal configuration of the receiving set 102 of the gestalt of this operation is described using drawing 3 .

[0045] That is, as shown in drawing 3 , D-IF1394 I/O means 102a performs I/O of an eye SOKURONO spa blanket and a ray synchronous packet between 1394 buses 105 and a receiving set 102. That is, D-IF1394 I/O means 102a is a means to output data packet 209a of an eye SOKURONO spa blanket which received from 1394 buses 105 to the packet decode means 301, and to output key information 203a of the ray synchronous packet which received from 1394 buses 105 to the key acquisition means 302. Moreover, D-IF1394 I/O means 102a is a means to output the key information transfer demand which the key acquisition means 302 outputs and which is a ray synchronous packet to 1394 buses 105.

[0046] The packet decode means 301 obtains data packet 209a from D-IF1394 I/O means 102a. Extract 2-bit data from the Sy field 910 (refer to drawing 6) among packets, and the contents of the 2 bit data are decoded. It is a means to send 2 bit data which extracted 2 extracted bit data when delivery and it showed the Inn-transition mode (modification information) to the mode detection means 303 also to the decryption means 304. Moreover, the packet decode means 301 is a means to send the live data 905 (to refer to drawing 6) of Uchi of a packet to the decryption means 304 or the data-logging playback means 305 according to the result of having decoded the contents of 2 bit data.

[0047] The mode detection means 303 investigates the contents of the copy management information sent from the packet decode means 301, and is a means to send the information on the purport which needs to receive the key for decode of live data 905 to the key acquisition means 302 according to the investigated result.
[0048] The key acquisition means 302 is a means to send the transfer request of the key information for starting acquisition of a key to D-IF1394 I/O means 102a, when the above-mentioned information has been sent from the mode detection means 303. In addition, an important thing is that the copy management information sent from the mode detection means 303 is attached to this transfer request here.
[0049] In addition, attachment of this copy management information may attach copy management information as it is, and after changing into a certain value, it may attach it. Predetermined changes, and when it attaches, the sending set 101 knows the Ruhr of conversion and can detect the copy management information before conversion. Conversion of changing 01 [2-bit] into 0100 [4-bit], and changing 10 into 0010 as an example of predetermined conversion, for example is carried out, and the configuration which sends these 4 bits can be considered.
[0050] Moreover, the key acquisition means 302 is a means to send key information 203a transmitted from the sending set 101 side to the key preservation means 306. In addition, the data control information detection means of this invention includes the packet decode means 301 and the mode detection means 303.
[0051] The key preservation means 306 is a means to save temporarily the key information sent from the key acquisition means 302, and to output the key information to the decryption means 304 to predetermined timing.
[0052] The decryption means 304 is a means to decrypt live data 905 using the key information from the key preservation means 306, and the modification information 310 on the key from the packet decode means 301.
[0053] AV data by which the data-logging playback means 305 was decrypted with the decryption means 304 -- or it is a means to indicate the AV data directly sent from the packet decode means 301 by delivery to the display means 307, and is a means to record on the record medium to build in. Moreover, the voice output means 308 is a means to output the voice data from the data-logging playback means 305.
[0054] In addition, it is the configuration same also about the other receiving sets 103-104 as the above.
[0055] The gestalt of 1 operation of the data transmitting approach of this invention and the data receiving approach is also explained [in / next / the above configuration] to coincidence, describing actuation of the gestalt of this operation referring to drawing 2 - drawing 4 .
[0056] Drawing 4 is drawing showing the temporal response of 2 bit data stored in the Sy field 910 (refer to drawing 6) of the gestalt of this operation, and a cryptographic key.
[0057] As shown in drawing 4 , with the gestalt of this operation, the sending set 101 shall have transmitted [the 1st AV data 401] the 3rd AV data 404 for voice data 403 from time of day T1 to T6 on 1394 buses 105 after that further among T7 till time of day T1 from the 2nd AV data 402 and time of day T6.
[0058] Moreover, these transfers copy-of-data management information is the ban on a copy, the one copy possibility of, a copy free-lancer, and the ban on a copy in an order from before, respectively as it is shown in this drawing. Therefore, as for a transfer of the 1st AV data 401, the 2nd AV data 402, and the 3rd AV data 404, Group B, Group A, and Group B correspond to this sequence, respectively as the correspondence relation between each transfer data and the group of the key to be used is shown in this drawing. Moreover, voice data 403 is a copy free-lancer, and the group who corresponds since it is not enciphered does not exist. Furthermore, updating (a key A1 - A3) of the cryptographic key shall be carried out 3 times in Group A during a transfer of the 2nd AV data 402 again.
[0059] (1) Describe the actuation immediately after time of day T1 first.
[0060] That is, the mode decision means 202 (refer to drawing 2) detects 2nd AV copy-of-data management information outputted from the data output means 201, decides the group of the cryptographic key corresponding to [carry out a thing judging and] it in whom one copy is possible to be A, and tells the key generating means 203. In Group A, the key generating means 203 creates a cryptographic key A1, and sends it to the key preservation means 204. The encryption means 205 enciphers the 2nd AV data 402 using the cryptographic key A1 sent from the key preservation means 204. The packet generation means

209 makes the 2nd enciphered AV data 402 live data 905, stores in the Sy field 910 "10" of the copy management information sent through the modification information generating means 208, and outputs it to D-IF1394 I/O means 101a as a data packet.
[0061] On the other hand, in a receiving set 102 (refer to drawing 3), the data packet containing the 2nd AV data 402 transmitted on 1394 buses 105 is received through D-IF1394 I/O means 102a.
[0062] the packet decode means 301 specifically extracts 2 bit data "10" which are storing, now the copy management information which is from the received data packet in the Sy field 910, and live data 905 are enciphered from the contents -- a thing judging is carried out. And the 2 above-mentioned bit data "10" are sent to the key acquisition means 302 as information on the purport which needs to receive the key for decode of live data 905. The key acquisition means 302 attaches 2 bit data "10" and the identification number of a sending set, and sends the transfer request of the key information for starting acquisition of a cryptographic key to D-IF1394 I/O means 102a. In addition, the identification number of a sending set is stored in the source ID 906 (refer to drawing 6).
[0063] In addition, there are two kinds of ways among the ways of attachment of the copy management information to a transfer request as mentioned above. It is the same when describing this below.
[0064] In a sending set 101 (refer to drawing 2), the transfer request of the key information from a receiving set 102 is received. The key distribution means 206 sends the 2 above-mentioned bit data "10" (copy management information) given to the transfer request to the key generating means 203, after passing through a predetermined authentication procedure with the dispatch origin of the above-mentioned transfer request. A . key generating means 203 by which this authentication procedure is procedure for a partner to judge whether it is a right device It investigates which are the code mode (namely, group of a key) corresponding to the "10", and the key with which it corresponds in the group. After judging that it is the key A1 in the group A of a key, it carries out whether the same key A1 which generates the key or is saved by already creating is obtained, and transmits to the dispatch origin of the above-mentioned transfer request. In addition, we decided to investigate the group of the key corresponding to it, and the cryptographic key in that group using the 2 above-mentioned bit data "10" (copy management information) specially given to this appearance at the transfer request, without the key distribution means 206 transmitting the cryptographic key A1 saved for the key preservation means 204 as it is for preventing the malfeasance stated in the column of the conventional technical problem. About this, it mentions later further.
[0065] On the other hand, in a receiving set 102 (refer to drawing 3), the key acquisition means 302 obtains the cryptographic key A1 transmitted from the sending set 101 side, and sends to the key preservation means 306. The decryption means 304 decodes the enciphered data which were obtained from the key preservation means 306 and which have been sent from the packet decode means 301 using a cryptographic key A1, and sends them to the data-logging playback means 305.
[0066] The data-logging playback means 305 judges that one copy is possible for the data "10" stored in the Sy field 910, and it outputs it also to the display means 307 and the voice output means 308 at coincidence, recording 2nd AV data decrypted by the record medium to build in.
[0067] Here, when recording 2nd AV data, the data-logging playback means 305 performs the above-mentioned record actuation, after rewriting with "11" the data of "10" which is the copy management information stored in the Sy field 910. It is because it means that, as for this, the copy was performed once by the above-mentioned record and the copy of after that from the record medium should forbid. However, rewriting of the copy management information contained in live data 905 is not performed. In addition, since it is changing, even if a receiving set 102 is made not to encipher for a while from transmitting initiation of 2nd AV data, it is easy to be natural [what the cryptographic key was using just before that / a receiving set] in T1 time of day when 2nd AV data transfer is started, in order to avoid the problem that 2nd AV data cannot be decoded until it receives a key new as mentioned above. Here, in while it is for a while, it is until acquisition of a new key is completed to a receiving set 102 side.
[0068] (2) Next, describe the actuation in time of day T2 - T3.
[0069] In the meantime, the modification information "01" which shows the Inn-transition mode is stored in the Sy field 910. The packet decode means 301 of a receiving set 102 will announce beforehand the purport which has renewal of delivery and a key in the modification information "01" to the decryption

means 304, if it detects that 2 bit data "01" are stored in the Sy field 910, and the decryption means 304 starts preparation of new decode processing. Moreover, the mode detection means 303 detects that the 2 above-mentioned bit data "01" are modification information, and tells a purport [need / a new key / to be received] to the key acquisition means 302. Here, copy management information is needed as mentioned above on the occasion of the transfer request of the new key of a schedule changed after predetermined time. However, since copy management information is not stored in the Sy field 910 in this case, "10" of the copy management information sent to beforehand [direct] the information on the Inn-transition mode sent is used. Therefore, to a sending set 101, the key acquisition means 302 attaches "10" of the last copy management information, and advances the transfer request of the above-mentioned key.
[0070] In addition, since the group of a key is not changed, it does not matter as a configuration which does not send "10" of copy management information.
[0071] on the other hand -- a sending set 101 -- the key distribution means 206 -- the above -- in response to the transfer request of a new key, generation of the new key A2 of the schedule used from time-of-day T3 determined by the change timing decision means 207 is required of the key generating means 203, and the generated new key A2 is transmitted to a receiving set 102 side. In time of day T1, the sending set 101 which received the transfer request of the key information from a receiving set 102 . which was performing predetermined authentication procedure with the dispatch origin of the above-mentioned transfer request before transmitting a key to the dispatch origin of a transfer request, since authentication procedure is already completed to this appearance . which does not need to perform authentication procedure again before a transfer of a key this time from time of day T2 to time-of-day T3 namely, -- -- in addition, the generated key A2 is sent also to the key preservation means 204. Moreover, as a result of a predetermined exchange, the key distribution means 206 checks that distribution of the key to a receiving set 102 has been completed, changes completion information of distribution 206a, and sends it to the timing decision means 207. The change timing decision means 207 directs to encipher by changing the key which was being used till then into the new key A2 obtained from the key preservation means 204 to the encryption means 205, after acquiring the completion information of distribution. Thereby, from time-of-day T3, the 2nd AV data 402 enciphered by the cryptographic key A2 is transmitted on 1394 buses 105 as a data packet.
[0072] the 2nd AV data 402 enciphered by the cryptographic key A2 since the new key A2 had already carried out the completion of acquisition in the receiving set 102 side -- a data packet -- ** -- even when it receives by carrying out, it can decode satisfactory. Subsequent actuation is the same as that of the case of (1) mentioned above.
[0073] (3) Next, describe the actuation in time-of-day T-four-T5.
[0074] In this case, except for the point that a new key is key A3, it is the same as that of the above (2).
[0075] In addition, we decided to update a cryptographic key with time amount in the same mode in this way for securing the safety of encryption further. That is, the chance of decode of the code by the malfeasance increases, so that the time of the same key becomes long.
[0076] It takes into consideration that the accumulated dose of the encryption data based on the same key also becomes large, and damage when a code is decoded unjustly also becomes large temporarily on the other hand.
[0077] (4) Next, describe the actuation in time of day T6.
[0078] In this case, since a transfer of a copy free-lancer's voice data 403 is started in time of day T6, a cryptographic key does not exist. Therefore, just before time of day T6, the modification information "01" as above preliminary announcements is not taken out.
[0079] In a receiving set 102, it detects that "00" is stored in the Sy field 910 of a data packet where the packet decode means 301 was received, and live data 905 judge with not being enciphered and send live data 905 to the data-logging playback means 305 directly. Moreover, the transfer request of a key to a sending set 101 is not performed, either. Actuation with the data-logging playback means 305 is the same as that of the contents mentioned above.
[0080] (5) Next, describe the actuation in time of day T7.
[0081] In this case, since the data for a transfer are the 3rd AV data 404 and this is data of the ban on a copy, activity is the same as the case of the above (1). In addition, from the main point of preventing decode of the inaccurate code mentioned above with the gestalt of this operation, it is not concerned with

whether each is separately independent or each is discontinuous in time in the transfer data with which the same copy management information is given, but a cryptographic key is updated with time amount, and it has changed into key B-2 also here from the key B1 used for encryption of the 1st AV data 401. However, it belongs to the group B same [the group of a key] also as a key B1 and key B-2.

[0082] By the way, even if it alters copy management information, the point that the malfeasance beyond it can be prevented is stated to a detail, as the case where 3rd AV data was received was taken and mentioned above for the example.

[0083] That is, a malfeasance is performed by somewhere on 1394 buses 105, and the case where "11" information on Sy field is altered by "10" is considered in the 3rd AV data 404 which the receiving set 102 received.

[0084] The key acquisition means 302 (refer to drawing 3) attaches this data of altered "10", and performs the transfer request of the above-mentioned key as it was mentioned above. It judges that a key distribution means 206 (refer to drawing 2) by which this transfer request was obtained is a key which delivery and the key generating means 203 investigate the group of the key corresponding to "10" for "10" attached, and the cryptographic key in that group to the key generating means 203, and belongs to Group A, the key belonging to Group A is generated, and it is sent to a receiving set 102. The decryption means 304 of a receiving set 102 cannot perform right decode, even if it uses the key belonging to Group A for decode of the 3rd AV data 404. An original key is because it is key B-2 belonging to Group B.

[0085] Therefore, although the data-logging playback means 305 records only once the data in the incomprehensible condition of not decoding correctly on a record medium as the contents of copy management information "10", such record data do not have value in use, and a malfeasance turns into a useless action. Moreover, a display for the display means 307 will also be an incomprehensible image in this case. In addition, about the data which were not decoded correctly, even if it constitutes the data-logging playback means 305 in the appearance which does not perform record actuation, it is easy to be natural.

[0086] In addition, with the gestalt of the above-mentioned implementation, although the class of encryption of this invention was a cryptographic key, it may be the algorithm of not only this but a code. In this case, it becomes the configuration of changing the algorithm of the code applied to transmission of the above-mentioned data according to the management information of the data used as the candidate for transmitting. Moreover, it specifically, for example, greatly, divides as how to change the algorithm, and there are two kinds of following ways. Namely, other one changes the algorithm of a code by changing the loop count of encryption procedure by one changing the algorithm of a code by replacing the sequence of encryption procedure. The 1st encryption processing is applied and the property that the encryption data at the time of applying the 2nd encryption processing further to the processing result differ from the encryption data at the time of applying the sequence of the above 1st and the 2nd encryption processing conversely is used to the case of the former, for example, predetermined data, and it can realize, without complicating the configuration of hardware, such as an encryption circuit. In addition, the reinforcement of the code of both encryption data is the same level in this case. Moreover, although the count of a repeat of actuation of applying the 1st encryption processing and applying the still more nearly same encryption processing to that result to the case of the latter, for example, predetermined data, is generally called loop count, encryption data are changed by changing this loop count. In addition, the reinforcement of a code goes up what generally made [many] loop count in this case. Moreover, the configuration of changing the sequence of encryption procedure as what had combined the former and the latter, and needless to say also changing the loop count of each encryption processing may be used. Furthermore, in the above-mentioned case, a cryptographic key may be the same and may be changed again. When applying the configuration described above of changing the algorithm of a code, as decryption information which a sending set should transmit to a receiving set side, in the case of the former, it is the sequence of encryption processing for example, and, in the case of the latter, is loop count.

[0087] Moreover, the gestalt of the above-mentioned implementation explained rewriting the copy management information stored in Sy field in the case of record of the data with which one copy of a data-logging playback means is enabled. Here, the point is described further. The copy [which was stated also with the gestalt of the above-mentioned implementation] management information in which the data-

logging playback means is included in live data like does not rewrite. Therefore, since the information in Sy field and the information in live data are not in agreement when the record data is transmitted to another recording apparatus etc. after that, it is also considered that derangement arises in the another recording apparatus. Then, although both information should originally be made in agreement, in order to avoid that the configuration of equipment becomes complicated, it is good also as a configuration which writes in the information which dares allow an inequality condition, instead shows that to Sy field. That is, although the copy management information in live data is not rewriting in case it transmits after receiving and recording the data in which one copy is possible, as information which shows that the copy of live data is prohibition, a "stream copy" is newly named and 2 bit data stored in Sy field are set to "01." In this case, when recording AV data, the data-logging playback means 305 performs the above-mentioned record actuation, after rewriting the data of "10" which is the copy management information stored in the Sy field 910 with "01" which means the ban on the further copy. This becomes distinguishable [the data that it is the ban on a copy from the first as copy management information in the equipment of normal, and the data that a subsequent copy is prohibition since the copy was performed once]. Therefore, it becomes possible using the information in Sy field to make it operate correctly without derangement. Furthermore, the class (for example, the group C of a cryptographic key) of new encryption corresponding to the "stream copy" as copy management information can be established again by the same configuration as what was stated with the gestalt of the above-mentioned implementation in this case. That is, when there is equipment which transmits the record data (data of the second generation) further after the data in which one copy is possible were received and recorded as mentioned above, it is because the same effectiveness as the above can be demonstrated also about the copy-of-data management information of the second generation.

[0088] Moreover, since the Inn-transition information stated with the gestalt of the above-mentioned implementation in this case cannot be expressed, it is good in Sy field also as a configuration which secures as 1 bit which became independent to field where the Sy field 910 in the eye SOKURONOSU packet header 900 is another, and is stored there, for example.

[0089] Moreover, although the gestalt of the above-mentioned implementation described the case where the Inn-transition information "01" was stored in the SY field 910, not only this but the Sy field 910 in the eye SOKURONOSU packet header 900 is good also as a configuration which secures 1 bit which became independent to another field, and is stored there.

[0090] Moreover, with the gestalt of the above-mentioned implementation, after the receiving set received the preliminary announcement information on the key which changes with time amount, the case where the transfer request of a new key was advanced was stated. However, the configuration of sending to coincidence not only this but the key the above-mentioned sending set is due to use for a degree in addition to the key of which the transfer was required when a sending set has the transfer request of a key from the receiving set which transmitted update information instead of the above-mentioned preliminary announcement information, and received the update information may be used. Here, when the class (namely, class of encryption) of key is updated with time amount as mentioned above, the above-mentioned update information is the information for notifying to a receiving set that the updating was performed, and is generated by the modification information generating means 208 (refer to drawing 2). In addition, the updating execution information generation means of this invention is equivalent to this modification information generating means 208.

[0091] In this case, as shown in drawing 5 , the Inn-transition information that independent 1 bit was secured will be equivalent to the above-mentioned update information, and will tell a receiving set about the timing which uses a new key.

[0092] That is, in drawing 5 , if the receiving set has received the key A1 and the key A2 to coincidence immediately after time of day T1 and the Inn-transition information is reversed from 0 to 1 at the time of time-of-day T3, the receiving set which detected the timing of this reversal will start use of a new key (key A2). Moreover, the transfer request of a key is performed as the receiving set was mentioned above to the sending set at this time. The key A2 current in use and key A3 which is due to be used for a degree are sent to coincidence from a sending set to this transfer request. Therefore, what was already sent will be overlapped about a key A2. Then, although a receiving set holds this about key A3, about a key A2, the already acquired key is used for it as it is, and the key A2 sent to the 2nd times is thrown away. In addition,

it is easy to be natural even if it uses the already acquired key unlike this, substituting it for the key A2 sent to the 2nd times.
[0093] Moreover, in drawing 5 , at time of day T5, since it is reversed to 1-0, after detecting this reversal, it becomes the same actuation as the above. Of course, the above-mentioned contents can be similarly applied, even when changing the algorithm of not only a cryptographic key but a code.
[0094] Moreover, although the key was transmitted as it was as decryption information with the gestalt of each above-mentioned operation implementation in order to simplify explanation . which may be what kind of information as long as it is the information to which decryption information is not restricted to this and a receiving set can create a key -- for example So that may encipher a key, it may transmit to a receiving set, a receiving set may decrypt the enciphered key and the key itself may come to hand . which may be carried out . which may share information required for this decryption between a sending set and a receiving set in the case of authentication procedure, or may be beforehand stored in a sending set and a receiving set at the time of equipment manufacture -- if it does in this way, even if intercepted by the 3rd person, a key will not cross transmission of a key to the 3rd person.
[0095] Moreover, although the case where an encryption key was changed with time amount also about the data of the same copy management information was described, if it is the configuration of changing a key and the algorithm of encryption for example, not only according to this but according to copy management information, even if it does not make it differ in time, it will be available [the gestalt of the above-mentioned implementation].
[0096] Moreover, although the gestalt of the above-mentioned implementation described the case where a copy free-lancer, the one copy possibility of, the ban on a copy, etc. were used, as copy management information, even if there are some from which for example, not only this but the count of a copy differs, it is easy to be natural and does not restrict to these.
[0097] Moreover, record media which recorded the program for making a computer perform the function of the gestalt of the operation described above and the means of all or a part of each means given in any one example of those modifications, such as a magnetic-recording medium and an optical recording medium, can be created, and the same actuation as the above can be performed by using it.
[0098] Moreover, using a computer, the gestalt of the above-mentioned implementation and processing actuation of each means of those modifications may be realized by software by work of a program, or may realize the above-mentioned processing actuation in hardware by circuitry characteristic [without using a computer].
[0099]
[Effect of the Invention] This invention has the advantage in which protection of transmission data can carry out much more certainly compared with the former so that clearly from the place described above.

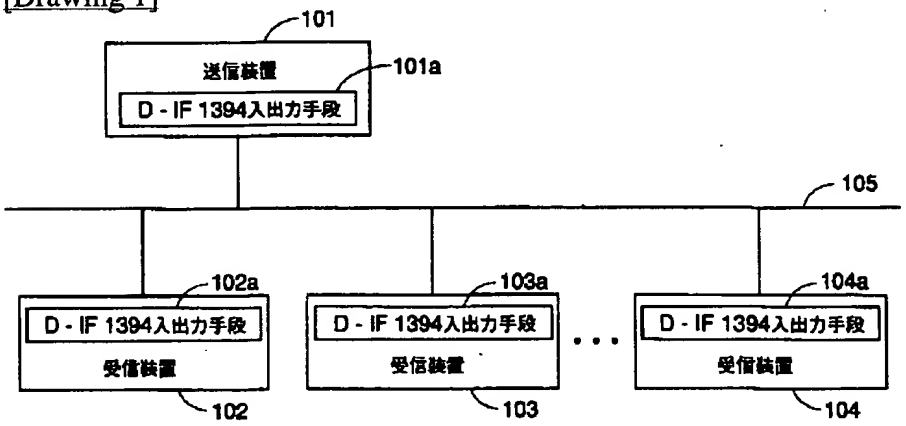
[Translation done.]

* NOTICES *

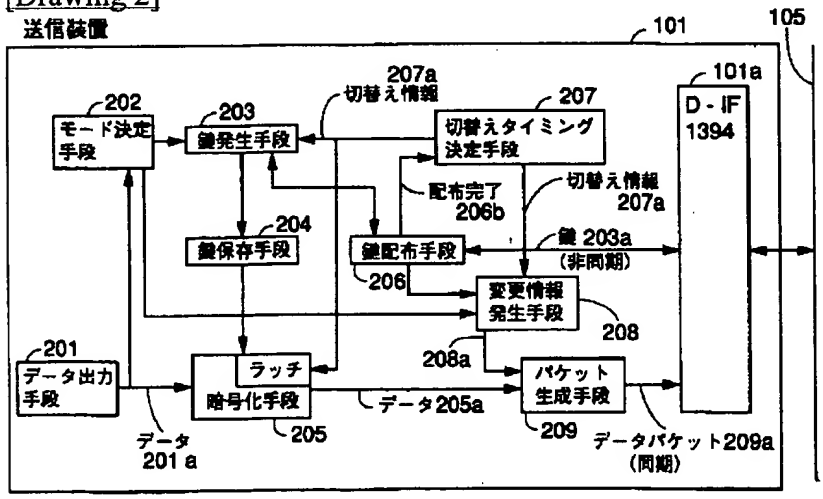
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

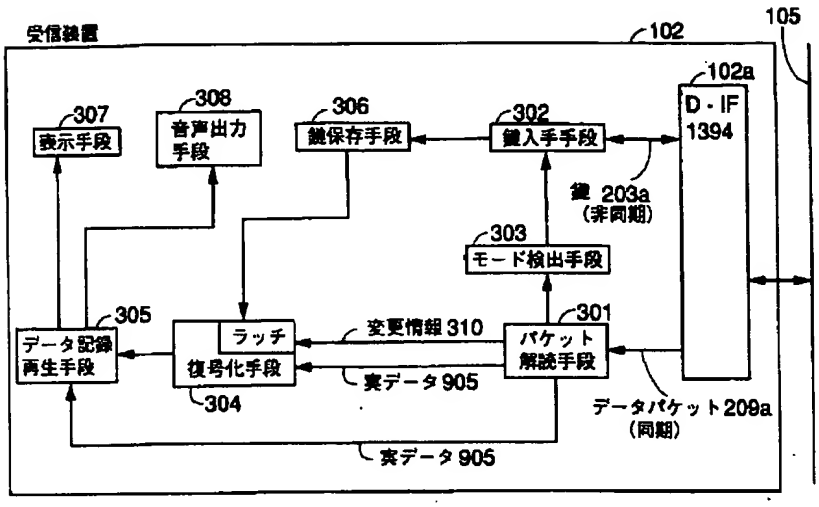
[Drawing 1]



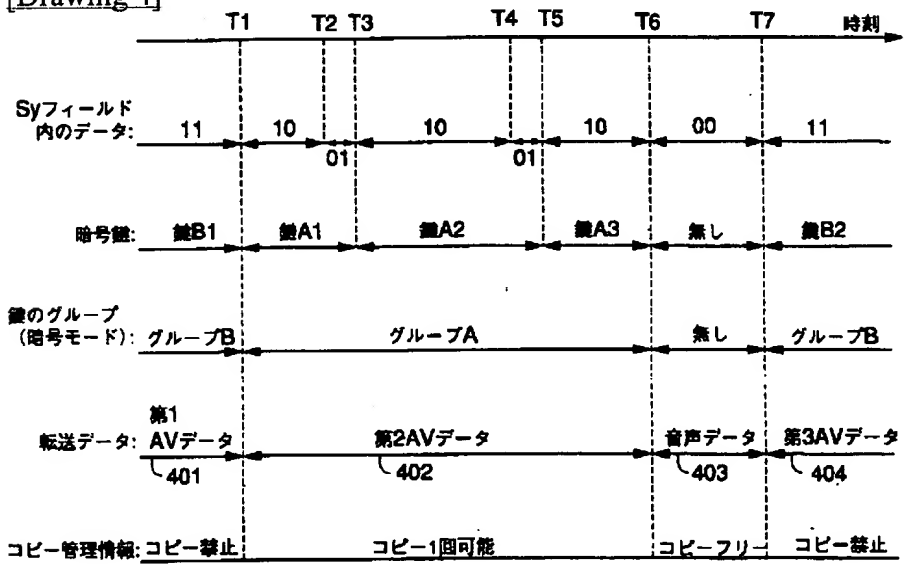
[Drawing 2]



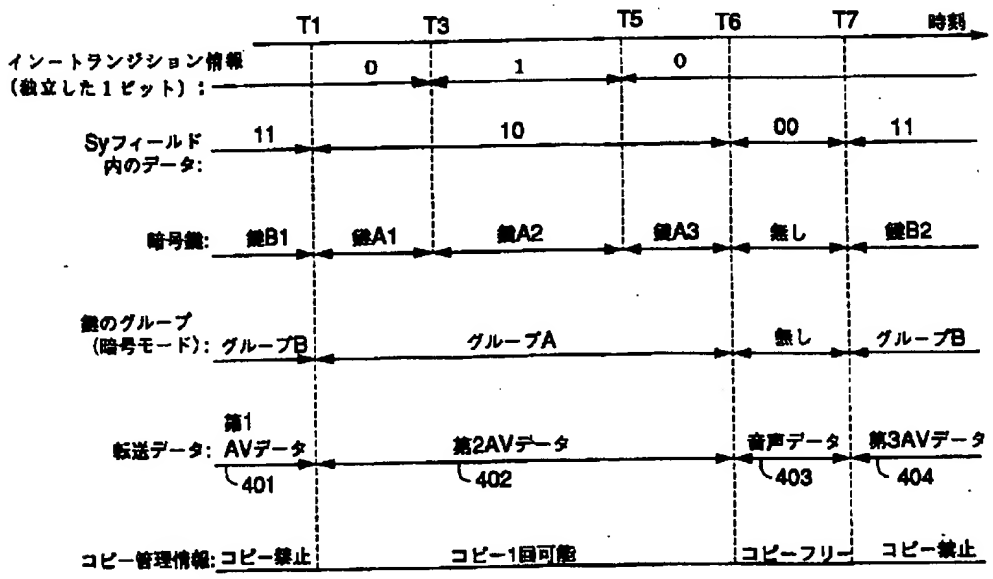
[Drawing 3]



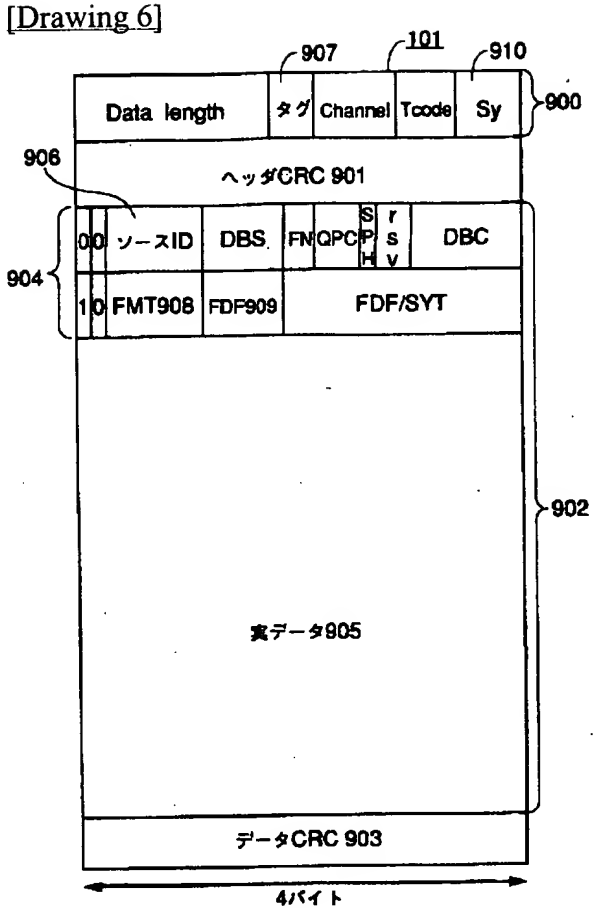
[Drawing 4]



[Drawing 5]



[Drawing 6]



[Translation done.]

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-205310
(43)Date of publication of application : 30.07.1999

(51)Int.CI. H04L 9/36
H04L 9/14
H04L 12/40

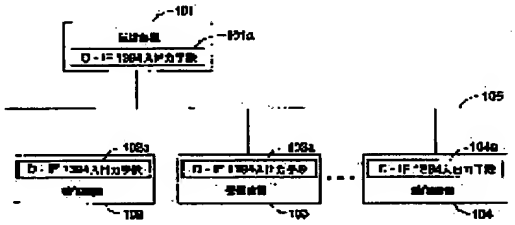
(21)Application number : 10-307358
(22)Date of filing : 28.10.1998

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : IIZUKA HIROYUKI
YAMADA MASAZUMI
TAKECHI HIDEAKI
MATSUZAKI NATSUME

(30)Priority
Priority number : 09297614 Priority date : 29.10.1997 Priority country : JP

(54) DATA TRANSMISSION METHOD, DATA RECEPTION METHOD, DATA TRANSMISSION SYSTEM AND PROGRAM RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To further surely protect transmission data by deciding the kind of ciphering to be applied corresponding to the management information of data, enciphering the data and transmitting them together with management information.
SOLUTION: The mode decision means of a transmitter 101 decides the group of a cryptographic key to be used corresponding to the contents of the copy management information of video data or the like to be transmitted and outputs it to a key generation means as cipher mode information. The key generation means generates a key to be used for enciphering within the decided group (A or B) of the key, based on it. When information is sent from a mode detection means, the key obtaining means of a receiver 102 sends the transfer request of key information for starting the obtaining of the key to a D-IF1394 input/output means 102a. The key obtaining means sends the key information transferred from the side of the transmitter 101 to a key preservation means and it is temporarily preserved there and outputted to an enciphering means. The deciphering means deciphers actual data by utilizing the key information from the key preservation means and key change information from a packet decoding means.



LEGAL STATUS

[Date of request for examination] 16.08.2001
[Date of sending the examiner's decision of rejection] 27.10.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

6

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－205310

(43)公開日　平成11年(1999)７月30日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/36		Ｈ０４Ｌ　9/00	６８５
9/14			６４１
12/40		11/00	３２０

審査請求　未請求　請求項の数31　ＯＬ　（全 15 頁）

(21)出願番号　特願平10－307358

(22)出願日　平成10年(1998)10月28日

(31)優先権主張番号　特願平9－297614

(32)優先日　平９(1997)10月29日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　飯塚　裕之
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　山田　正純
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　武知　秀明
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　松田　正道

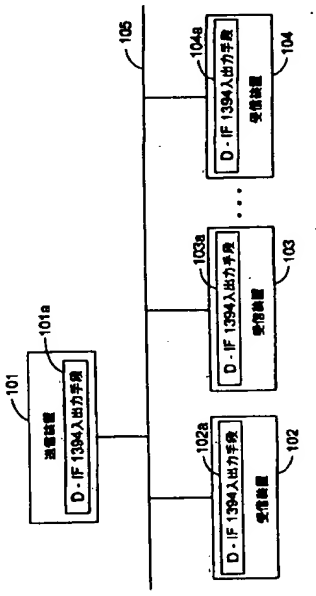
最終頁に続く

(54)【発明の名称】　データ送信方法、データ受信方法、データ伝送システム、及びプログラム記録媒体

(57)【要約】

【課題】コピー管理情報の改竄により復号化された実データが不正記録される。

【解決手段】送信データの管理情報に応じて送信データに適用する暗号鍵を決定するモード決定手段２０２と、その決定された鍵により送信データを暗号化する暗号化手段２０５と、暗号化されたデータとデータ管理情報とを送信する１３９４入出力手段１０１ａと、送信されてきた送信データを受信する１３９４入出力手段１０２ａと、その受信データからデータ管理情報を検出するパケット解読手段３０１と、送信データの送信元に対して、検出したデータ管理情報を送り、且つ、その送信したデータ管理情報に対応する鍵を要求する鍵入手手段３０２と、鍵の送信要求があった場合、データ管理情報に対応した鍵を要求元に送信する鍵配布手段２０６と、送信されてきた鍵により受信データを復号化する復号化手段３０４等を備える。



1

【特許請求の範囲】

【請求項１】　送信対象となるデータの管理情報に応じて前記データの送信に適用する暗号化の種類を決定し、
その決定された暗号化の種類に基づいて、前記データを暗号化し、
前記暗号化されたデータと前記データ管理情報とを送信することを特徴とするデータ送信方法。

【請求項２】　請求項１記載のデータ送信方法により送信されてきた送信データを受信し、
その受信データから前記データ管理情報を検出し、
前記送信データの送信元に対して、前記検出したデータ管理情報を送り、且つ、その送信したデータ管理情報に対応する復号化情報を要求することを特徴とするデータ受信方法。

【請求項３】　請求項２記載のデータ受信方法により前記復号化情報の要求があった場合、前記データ管理情報に対応した前記復号化情報を前記要求元に送信することを特徴とする請求項１記載のデータ送信方法。

【請求項４】　請求項３記載のデータ送信方法により送信されてきた前記復号化情報に基づいて、前記受信データを復号化し、
前記検出されたデータ管理情報に応じて、前記復号化した受信データの処理の仕方を決定することを特徴とする請求項２記載のデータ受信方法。

【請求項５】　前記データ管理情報が同一の場合であっても、前記暗号化の種類を時間と共に更新し、
前記送信対象となるデータを前記更新された暗号化の種類により暗号化し、
前記暗号化されたデータを送信する以前に、前記更新を行うことを予告する予告情報を送信することを特徴とする請求項１又は３記載のデータ送信方法。

【請求項６】　前記データ管理情報が同一の場合であっても、前記暗号化の種類を時間と共に更新し、
前記更新を行ったことを示す情報を送信し、
前記データ管理情報に対応する復号化情報の要求があった場合、その時点で使用されるべき復号化情報と、次の時点で使用される予定の復号化情報との双方を送信することを特徴とする請求項１又は３記載のデータ送信方法。

【請求項７】　前記暗号化の種類を時間と共に更新する場合、その更新された前記暗号化の種類が、前記データ管理情報に応じて決定された前記他の暗号化の種類と重複しないことを特徴とする請求項５又は６記載のデータ送信方法。

【請求項８】　請求項５記載のデータ送信方法により送信されてきた前記予告情報を受信した場合、その予告情報に応じて、前記送信データの送信元に対して前記復号化情報を要求することを特徴とする請求項２又は４記載のデータ受信方法。

【請求項９】　請求項６に記載のデータ送信方法により

2

送信されてきた前記更新を行ったことを示す情報を受信した場合、その受信した情報に基づいて、前記情報の送信元に対して、前記復号化情報を要求することを特徴とする請求項２又は４記載のデータ受信方法。

【請求項１０】　前記データ管理情報を送るとは、前記検出したデータ管理情報をそのまま送る、又は、前記検出したデータ管理情報を所定の変換を行って送ることであることを特徴とする請求項２又は８記載のデータ受信方法。

【請求項１１】　前記データ管理情報に応じて前記データの送信に適用する暗号化の種類を決定するとは、前記データ管理情報に応じて暗号化に用いる鍵を異ならせることであることを特徴とする請求項１又は３記載のデータ送信方法。

【請求項１２】　前記データ管理情報に応じて前記データの送信に適用する暗号化の種類を決定するとは、前記データ管理情報に応じて暗号化に用いるアルゴリズムを異ならせることであることを特徴とする請求項１又は３記載のデータ送信方法。

【請求項１３】　前記データ管理情報とは、前記データがコピー自由であるのか、１回コピー可能であるのか、又はコピー禁止であるのかを示す情報を含むコピー管理情報であることを特徴とする請求項１，３，５又は６記載のデータ送信方法。

【請求項１４】　前記コピー禁止であることを示す情報には、元からコピー禁止であることを示す情報と、元々１回コピー可能であったが、その１回のコピーが実行されたためにその後のコピーが禁止となったことを意味する更なるコピー禁止を示す情報との２種類の情報が含まれており、
前記暗号化の種類は、それら２種類の情報に応じて異なることを特徴とする請求項１３記載のデータ送信方法。

【請求項１５】　請求項１３記載のデータ送信方法により送信されてきたデータ管理情報が、１回コピー可能であることを示している場合、
前記１回コピー可能であることを示す情報をデータ管理情報として有するデータを所定の記録媒体に記録する際、そのデータ管理情報を前記１回コピー可能からコピー禁止を示す内容に変更し、そのコピー禁止を示すデータ管理情報と共に前記記録を行うことを特徴とする請求項８又は９に記載のデータ受信方法。

【請求項１６】　請求項１４記載のデータ送信方法により送信されてきたデータ管理情報が、１回コピー可能であることを示している場合、
前記１回コピー可能であることを示す情報をデータ管理情報として有するデータを所定の記録媒体に記録する際、そのデータ管理情報を前記１回コピー可能から前記更なるコピー禁止を示す内容に変更し、その更なるコピー禁止を示すデータ管理情報と共に前記記録を行うことを特徴とする請求項８又は９に記載のデータ受信方法。

【請求項１７】　送信対象となるデータの管理情報に応じて前記データの送信に適用する暗号化の種類を決定するモード決定手段と、
その決定された暗号化の種類に基づいて、前記データを暗号化する暗号化手段と、
前記暗号化されたデータと前記データ管理情報とを送信するデータ送信手段と、
前記データ送信手段により送信されてきた送信データを受信するデータ受信手段と、
その受信データから前記データ管理情報を検出するデータ管理情報検出手段と、
前記送信データの送信元に対して、前記検出したデータ管理情報を送り、且つ、その送信したデータ管理情報に対応する復号化情報を要求する復号化情報要求手段と、
前記復号化情報の要求があった場合、前記データ管理情報に対応した前記復号化情報を前記要求元に送信する復号化情報送信手段と、
前記送信されてきた前記復号化情報に基づいて、前記受信データを復号化する復号化手段と、
前記検出されたデータ管理情報に応じて、前記復号化された受信データの処理の仕方を決定する処理方法決定手段と、を備えたことを特徴とするデータ伝送システム。

【請求項１８】　前記データ管理情報を送るとは、前記検出したデータ管理情報をそのまま送る、又は、前記検出したデータ管理情報を所定の変換を行って送ることであることを特徴とする請求項１７記載のデータ伝送システム。

【請求項１９】　前記データ管理情報に応じて前記データの送信に適用する暗号化の種類を決定するとは、前記データ管理情報に応じて暗号化に用いる鍵を異ならせることであることを特徴とする請求項１７記載のデータ伝送システム。

【請求項２０】　前記データ管理情報に応じて前記データの送信に適用する暗号化の種類を決定するとは、前記データ管理情報に応じて暗号化に用いるアルゴリズムを異ならせることであることを特徴とする請求項１７記載のデータ伝送システム。

【請求項２１】　前記データ管理情報が同一の場合であっても、前記暗号化の種類を時間と共に更新する暗号化種類更新手段と、
前記更新を行うことを予告するための予告情報を生成する予告情報生成手段とを備え、
前記暗号化手段が前記送信対象となるデータを前記暗号化する場合、前記更新された暗号化の種類により暗号化し、
前記生成された予告情報が、前記更新された暗号化の種類により暗号化されたデータを送信する以前に送信されることを特徴とする請求項１７記載のデータ伝送システム。

【請求項２２】　前記データ管理情報が同一の場合であっても、前記暗号化の種類を時間と共に更新する暗号化種類更新手段と、
前記更新を行ったことを通知するための更新情報を生成する更新実行情報生成手段とを備え、
前記暗号化手段が前記送信対象となるデータを前記暗号化する場合、前記更新された暗号化の種類により暗号化し、
前記更新された暗号化の種類により暗号化されたデータの送信が開始される際に、前記更新情報が送信されることを特徴とする請求項１７記載のデータ伝送システム。

【請求項２３】　前記復号化情報要求手段は、受信された前記予告情報に応じて、前記送信データの送信元に対して前記復号化情報を要求することを特徴とする請求項２１のデータ伝送システム。

【請求項２４】　前記復号化情報要求手段は、受信された前記更新情報の変化に応じて、前記送信データの送信元に対して、前記復号化情報を要求することを特徴とする請求項２２記載のデータ伝送システム。

【請求項２５】　前記暗号化の種類を時間と共に更新する場合、その更新された前記暗号化の種類が、前記データ管理情報に応じて決定された前記他の暗号化の種類と重複しないことを特徴とする請求項２１～２４の何れか一つに記載のデータ伝送システム。

【請求項２６】　前記データ管理情報とは、前記データがコピー自由であるのか、１回コピー可能であるのか、又はコピー禁止であるのかを示す情報を含むコピー管理情報であることを特徴とする請求項１７～２５の何れか一つに記載のデータ伝送システム。

【請求項２７】　前記コピー禁止であることを示す情報には、元からコピー禁止であることを示す情報と、元々１回コピー可能であったが、その１回のコピーが実行されたためにその後のコピーが禁止となったことを意味する更なるコピー禁止を示す情報との２種類の情報が含まれており、
前記暗号化の種類は、それら２種類の情報に応じて異なることを特徴とする請求項２６記載のデータ伝送システム。

【請求項２８】　前記データ送信手段により送信されてきたデータ管理情報が、１回コピー可能であることを示している場合、
前記１回コピー可能であることを示す情報をデータ管理情報として有するデータが所定の記録媒体に記録される際、そのデータ管理情報が、前記１回コピー可能からコピー禁止を示す内容に変更されて、そのコピー禁止を示すデータ管理情報と共に前記記録が行われることを特徴とする請求項２６に記載のデータ伝送システム。

【請求項２９】　前記データ送信手段により送信されてきたデータ管理情報が、１回コピー可能であることを示している場合、
前記１回コピー可能であることを示す情報をデータ管理

情報として有するデータが所定の記録媒体に記録される際、そのデータ管理情報が、前記１回コピー可能から前記更なるコピー禁止を示す内容に変更されて、その更なるコピー禁止を示すデータ管理情報と共に前記記録が行われることを特徴とする請求項２７に記載のデータ伝送システム。

【請求項３０】請求項１～１６の何れか一つに記載の各ステップの全部又は一部のステップをコンピュータに実行させるためのプログラムを記録したことを特徴とするプログラム記録媒体。

【請求項３１】請求項１７～２９の何れか一つの請求項に記載の各手段の全部又は一部の手段の機能をコンピュータに実行させるためのプログラムを記録したことを特徴とするプログラム記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えば、ディジタルデータを送受信する、データ送信方法、データ受信方法、データ伝送システム、及びプログラム記録媒体に関するものである。

【０００２】

【従来の技術】従来のデータ転送方式には、ＩＥＥＥ１３９４規格（IEEE: THE INSTITUTE OFELECTRICAL AND ELECTRINIC ENGINEERS, INC）を用いたデータ転送方法がある。（参考文献：IEEE1394 High Performance Serial Bus）ＩＥＥＥ１３９４規格におけるデータ転送には、映像信号や音声信号等の同期データの転送に適したアイソクロノス通信と、制御信号等の非同期データの転送に適したエイシンクロナス通信とがあり、両通信はＩＥＥＥ１３９４バス上で混在することが可能である。

【０００３】アイソクロノス通信は、いわゆる放送型の通信であり、ＩＥＥＥ１３９４バス上のある装置が出力するアイソクロノスパケットは、同バス上の全ての装置が受信することができる。

【０００４】これに対してエイシンクロナス通信は、１対１の通信と放送型通信の両方がある。そして、バス上のある装置が出力するエイシンクロナスパケットには、そのパケットを受信すべき装置をあらわす識別子が含まれており、その識別子が特定の装置をあらわす時にはその識別子で指定された装置が当該エイシンクロナスパケットを受信し、識別子がブロードキャストをあらわす時には同バス上の全ての装置が当該エイシンクロナスパケットを受信する。

【０００５】また、ＩＥＥＥ１３９４規格を用いてディジタル音声信号やディジタル映像信号等を転送したり、ＩＥＥＥ１３９４バス上につながれた機器間でデータ伝送経路の接続管理を行うための規格として、ＩＥＣ（IEC: InternationalElectrotechnical Commission 国際電気標準会議）においてＩＥＣ６１８８３規格（以下、ＡＶプロトコルと称する）が検討されている。ＡＶプロトコルにおいては、映像音声データはアイソクロノスパケット内に配置されて転送される。また、アイソクロノスパケットはＣＩＰヘッダ（CIP: Common Isochronous Packet）を含む。ＣＩＰヘッダ内には映像音声データの種類を示す識別情報や、アイソクロノスパケットを送信している送信装置の装置番号等の情報が含まれている。

【０００６】このような従来のデータ転送方式を用いたデータ伝送システムにおいて、送信対象となるデータの著作権保護の観点から、転送対象となるデータのコピーの制限をデータ保護情報により行えるデータ伝送システムが提案されている。この様に、コピー制限の仕組みが必要なディジタルデータとしては、例えば、映像をディジタル化したビデオデータや、音声をディジタル化したオーディオデータや、あるいは両方を合わせて構成されたディジタルデータなどがある。

【０００７】以下に、このような従来のデータ伝送システムについて、図６を参照しながらその構成を述べる。

【０００８】即ち、図６は、従来のデータ伝送システムにて使用されるアイソクロノスパケットのフォーマットをあらわす図である。

【０００９】同図に示す通り、アイソクロノスパケット１０１は、アイソクロノスパケットヘッダ９００、ヘッダＣＲＣ９０１、アイソクロノスペイロード９０２、データＣＲＣ９０３からなる。

【００１０】アイソクロノスパケットヘッダ９００には、データ保護情報を格納するためのＳｙフィールド９１０が含まれる。Ｓｙフィールド９１０の上位２ビットに格納された値が００である時には、送信対象となるデータ（後述する実データ９０５）が、コピーが自由に行えるデータである事を示している。また、１０である時には、そのデータが、１回のみコピー可能であることを、更に、１１である時には、そのデータが、コピー禁止であることを示している。

【００１１】又、アイソクロノスパケットヘッダ９００には2ビットのタグ９０７が含まれる。タグ９０７は、その値が０１である時には、そのアイソクロノスパケットがＡＶプロトコルに準拠したアイソクロノスパケットであることを示す。タグ９０７の値が０１であるとき、即ち、そのアイソクロノスパケットがＡＶプロトコル準拠のアイソクロノスパケットである時には、アイソクロノスペイロード９０２の先頭にＣＩＰヘッダ９０４が含まれる。

【００１２】ＣＩＰヘッダ９０４の中には、当該アイソクロノスパケットを出力している出力装置の識別子であるソースＩＤ９０６が含まれる。また、ＣＩＰヘッダ９０４には、アイソクロノスペイロード９０２に含まれる実データ９０５がどの様な種類のデータであるかをあらわすＦＭＴ９０８やＦＤＦ９０９が含まれる。

【００１３】映像や音声の送信対象となるデータは実データ９０５に含まれるが、この実データ９０５は、上述

したデータ保護情報が、１０又は１１である場合には、暗号化されたデータであるが、コピーフリーを意味する００の場合には、暗号化はされていない。又、データ保護情報は、実データ９０５中にも含まれており、一般に、ＣＤの場合はＳＣＭＳと、また、ＤＶの場合はＣＧＭＳ等と呼ばれている。

【００１４】このような構成において、次に動作を説明する。すなわち、送信機はディジタルデータを送信する際に、コピーしてよいかどうかの条件を示すデータ保護情報を、アイソクロノスパケットヘッダ９００のＳｙフィールド９１０に格納して、実データ９０５と共に送信する。受信機側は、受信したデータのＳｙフィールド９１０の中からデータ保護情報を検出して、データ保護情報の内容を解釈した結果に基づいて、ディジタルデータを記録するときの機器の動作を切り替える。又、コピーフリーのデータである場合を除いて、実データが暗号化されているので、受信機側は、それを復号化するために必要な復号化情報の転送を送信機側へ要求する。送信機は、その要求を受けて、復号化情報をその要求元へ送る。受信機は、送信機から送られてきた復号化情報を用いて、受信した実データ９０５を復号化する。この様にして復号化された実データ９０５は、表示装置に表示される。一方、その復号化された実データの記録動作に関しては、データ保護情報の内容に基づいて適宜切り替られる。

【００１５】即ち、受信機が、例えばＶＴＲであるならば、検出したデータ保護情報が、“コピー１回可能”を意味している場合、復号化されたデータがＶＴＲに内蔵されたビデオテープに記録される。又、“コピー禁止”を意味している場合、仮に録画ボタンが押されていたとしても、記録動作は行われない。

【００１６】

【発明が解決しようとする課題】しかし、このような従来のデータ伝送システムでは、不正行為を行おうとする者により、送信機側と受信機側の間の伝送路中において、Ｓｙフィールド９１０の中に格納されているデータ保護情報が改竄された場合、復号化されたデータが不正にコピーされてしまうという課題を有していた。

【００１７】即ち、例えば、送信機から送信された段階では、アイソクロノスパケットヘッダ９００のＳｙフィールド９１０の中に格納されているデータ保護情報の値が１１であり、“コピー禁止”を意味していた場合に、不正行為者が、伝送路において、そのデータ保護情報の値を“コピー１回可能”を意味する１０に改竄したとする。以下、この場合について更に具体的に説明する。

【００１８】即ち、この場合、受信機側のＶＴＲは、Ｓｙフィールド９１０の中に格納されているデータ保護情報を見て、その値が１０であることを検出する。この場合、実データ９０５は上述した様に暗号化されているので、それを復号化するための復号化情報の送信要求を送信機に対して送る。この要求を受けた送信機は、要求元の受信機に対して復号化情報を送る。受信機側は、送られてきた復号化情報を用いて、実データ９０５を復号化した上で、その復号化された実データを表示装置等に表示する。一方、ＶＴＲは、上述した通り、Ｓｙフィールド９１０の中に格納されているデータ保護情報の値が１０であることを検出しているので、受信した実データ９０５が、本来コピー禁止のデータであるにも関わらず、コピー１回可能と判断して、上記復号化された実データをビデオテープに録画してしまうという課題を有していた。

【００１９】本発明は、上記従来のデータ伝送システムのこの様な課題を考慮し、伝送データの保護が従来に比べてより一層確実に行えるデータ送信方法、データ受信方法、データ伝送システム、及びプログラム記録媒体を提供することを目的とする。

【００２０】

【課題を解決するための手段】第１の本発明（請求項１記載の発明に対応）は、送信対象となるデータの管理情報に応じて前記データの送信に適用する暗号化の種類を決定し、その決定された暗号化の種類に基づいて、前記データを暗号化し、前記暗号化されたデータと前記データ管理情報とを送信するデータ送信方法である。

【００２１】又、第２の本発明（請求項２記載の発明に対応）は、上記第１の本発明のデータ送信方法により送信されてきた送信データを受信し、その受信データから前記データ管理情報を検出し、前記送信データの送信元に対して、前記検出したデータ管理情報を送り、且つ、その送信したデータ管理情報に対応する復号化情報を要求するデータ受信方法である。

【００２２】又、第３の本発明（請求項３記載の発明に対応）は、上記第２の本発明のデータ受信方法により前記復号化情報の要求があった場合、前記データ管理情報に対応した前記復号化情報を前記要求元に送信する上記第１の本発明のデータ送信方法である。

【００２３】又、第４の本発明（請求項４記載の発明に対応）は、上記第３の本発明のデータ送信方法により送信されてきた前記復号化情報に基づいて、前記受信データを復号化し、前記検出されたデータ管理情報に応じて、前記復号化した受信データの処理の仕方を決定する上記第２の本発明のデータ受信方法である。

【００２４】又、第１７の本発明（請求項１７記載の発明に対応）は、送信対象となるデータの管理情報に応じて前記データの送信に適用する暗号化の種類を決定するモード決定手段と、その決定された暗号化の種類に基づいて、前記データを暗号化する暗号化手段と、前記暗号化されたデータと前記データ管理情報とを送信するデータ送信手段と、前記データ送信手段により送信されてきた送信データを受信するデータ受信手段と、その受信データから前記データ管理情報を検出するデータ管理情報

検出手段と、前記送信データの送信元に対して、前記検出したデータ管理情報を送り、且つ、その送信したデータ管理情報に対応する復号化情報を要求する復号化情報要求手段と、前記復号化情報の要求があった場合、前記データ管理情報に対応した前記復号化情報を前記要求元に送信する復号化情報送信手段と、前記送信されてきた前記復号化情報に基づいて、前記受信データを復号化する復号化手段と、前記検出されたデータ管理情報に応じて、前記復号化された受信データの処理の仕方を決定する処理方法決定手段と、を備えたデータ伝送システムである。

【００２５】又、第２１の本発明（請求項２１記載の発明に対応）は、上記データ管理情報が同一の場合であっても、前記暗号化の種類を時間と共に更新する暗号化種類更新手段と、前記更新を行うことを予告するための予告情報を生成する予告情報生成手段とを備え、前記暗号化手段が前記送信対象となるデータを前記暗号化する場合、前記更新された暗号化の種類により暗号化し、前記生成された予告情報が、前記更新された暗号化の種類により暗号化されたデータを送信する以前に送信される上記第１７の本発明のデータ伝送システムである。

【００２６】又、第２２の本発明（請求項２２記載の発明に対応）は、上記データ管理情報が同一の場合であっても、前記暗号化の種類を時間と共に更新する暗号化種類更新手段と、前記更新を行ったことを通知するための更新情報を生成する更新実行情報生成手段とを備え、前記暗号化手段が前記送信対象となるデータを前記暗号化する場合、前記更新された暗号化の種類により暗号化し、前記更新された暗号化の種類により暗号化されたデータの送信が開始される際に、前記更新情報が送信される上記第１７の本発明のデータ伝送システムである。

【００２７】以上の構成により、本発明は、伝送データの保護が従来に比べてより一層確実に行える。

【００２８】

【発明の実施の形態】以下、本発明のデータ伝送システムの一実施の形態について、図面を参照しながら説明する。

【００２９】図１は、本実施の形態のデータ伝送システムの全体を示した概略構成図であり、図２，３は、そのデータ伝送システムを構成する送信装置、および受信装置についての構成図である。

【００３０】以下、同図を用いて本実施の形態の構成について述べる。

【００３１】図１に示す様に、本実施の形態のデータ伝送システムは、送信装置１０１と、複数の受信装置１０２～１０４が、ＩＥＥＥ１３９４バス１０５によって接続されている。それぞれの装置１０１～１０４と、ＩＥＥＥ１３９４バス１０５との接続は、Ｄ－ＩＦ１３９４入出力手段（１０１ａ～１０４ａ）を介して行われている。

【００３２】又、送信装置１０１と、複数の受信装置１０２～１０４との間におけるデータ転送は、従来のデータ伝送システムについて説明したものと同様である。即ち、映像信号や音声信号等の同期データの転送に適したアイソクロノス通信と、制御信号等の非同期データの転送に適したエイシンクロナス通信とが、ＩＥＥＥ１３９４バス１０５上で混在可能な構成となっている。

【００３３】次に、図２を用いて、本実施の形態の送信装置１０１の内部構成を述べる。

【００３４】即ち、図２に示すように、データ出力手段２０１は、１３９４バス１０５上に送信しようとする所定長の映像データ等をモード決定手段２０２及び暗号化手段２０５に対して出力する手段である。モード決定手段２０２は、送信しようとする映像データ等のコピー管理情報の内容に応じて、暗号化の鍵としてどのグループの鍵を用いるかを決定し、その決定された内容を暗号モード情報として鍵発生手段２０３に出力する手段である。コピー管理情報と暗号化モードとの対応は更に後述する。本実施の形態では、コピー管理情報は、コピーフリー、コピー１回可能、及びコピー禁止の３種類の著作権の保護のレベルを示す情報であるとする。本実施の形態のコピー管理情報は、本発明のデータ管理情報に対応する。また、鍵発生手段２０３は、モード決定手段２０２からの暗号モード情報に従って、決定された鍵のグループ（グループＡ又は、Ｂ）内において、暗号化に用いる鍵２０３ａを発生させる手段である。この鍵の発生は、切り替えタイミング決定手段２０７からの切り替え情報２０７ａに応じて時間的に順次行われるものであり、且つ、発生された鍵は全て異なる。

【００３５】ここで、上述した通り、コピー管理情報と暗号化モードとの対応について更に述べる。

【００３６】即ち、本実施の形態では、上記３種類のコピー管理情報に対応して、コピーフリーでは、暗号化を行わないものとし、コピー１回可能では暗号鍵はグループＡの中から決定され、又、コピー禁止では暗号鍵はグループＢの中から決定されるものとする。換言すれば、暗号化モード情報は、暗号鍵のグループを識別する情報である。尚、グループＡとグループＢとは、共通する鍵を持たないとする。

【００３７】又、鍵保存手段２０４は、鍵発生手段２０３により発生された鍵２０３ａを一時的に保存し、保存している鍵２０３ａを暗号化手段２０５に出力する手段である。暗号化手段２０５は、データ出力手段２０１から出力されてきた映像データ２０１ａを鍵保存手段２０４から送られてきた鍵２０３ａを用いて暗号化し、暗号化データ２０５ａをパケット生成手段２０９に出力する手段である。鍵配布手段２０６は、受信装置からの要求に応じて、要求元の認証作業及びその認証結果に基づく鍵２０３ａの配布を非同期通信により行い、又、鍵２０３ａの配布の完了した旨を切り替えタイミング決定手

段２０７に送る手段である。切り替えタイミング決定手段２０７は、上述した様に、モード決定手段２０２により決定された鍵のグループ内において、時間とともに暗号化に用いる鍵を更新していくための、鍵の切り替え時期を決定する手段であり、その切り替え時期を示す切り替え情報２０７ａを鍵発生手段２０３及び変更情報発生手段２０８に送る手段である。変更情報発生手段２０８は、鍵配布手段２０６、切り替えタイミング決定手段２０７からの情報を得て、インートランジション　モード情報を作成する手段であり、モード決定手段２０２から送られてくるコピー管理情報（暗号モードと対応）とインートランジションモード情報とを選択的にパケット生成手段２０９へ出力する手段である。

【００３８】ここで、インートランジションモード情報とは、同一の暗号モード内において、鍵が切り替えられるタイミングを事前に予告するための情報である。

【００３９】又、本実施の形態では、暗号モード情報とインートランジションモード情報は、いずれも図６で述べたアイソクロノスパケットヘッダ９００内のＳｙフィールド９１０に格納されるもので、２ビットからなるデータ２０８ａである。

【００４０】又、この２ビットデータ２０８ａのパターンと、コピー管理情報（暗号モード情報と対応）及びインートランジションモード情報との対応は、次の通りである。

【００４１】即ち、コピー管理情報がコピーフリーでは００、コピー１回可能では１０、コピー禁止では１１とし、インートランジションモードには０１を当てはめるものとする。

【００４２】パケット生成手段２０９は、暗号化データ２０５ａ（図６の実データ９０５に対応）と、Ｓｙフィールドに格納される２ビットデータ２０８ａとを得て、同期通信によりデータバス１０５上へ送信されるデータパケット２０９ａを生成し、それをＤ－ＩＦ１３９４入出力手段１０１ａに出力する手段である。尚、本実施の構成では、データパケットの構成は、図６で述べた構成と基本的に同じである。

【００４３】又、Ｄ－ＩＦ１３９４入出力手段１０１ａは、１３９４バス１０５と送信装置１０１との間でアイソクロノスパケットおよびエイシンクロナスパケットの入出力を行う。すなわち、パケット生成手段２０９の出力するデータパケット２０９ａ（アイソクロノスパケット）、および鍵配布手段２０６の出力する鍵情報２０３ａ（エイシンクロナスパケット）を１３９４バス１０５上に出力するとともに、１３９４バス１０５から受信したエイシンクロナスパケットを鍵配布手段２０６へと出力する手段である。

【００４４】次に、図３を用いて、本実施の形態の受信装置１０２の内部構成を述べる。

【００４５】即ち、図３に示す様に、Ｄ－ＩＦ１３９４

入出力手段１０２ａは、１３９４バス１０５と受信装置１０２との間でアイソクロノスパケットおよびエイシンクロナスパケットの入出力を行う。すなわち、Ｄ－ＩＦ１３９４入出力手段１０２ａは、１３９４バス１０５から受信したアイソクロノスパケットのデータパケット２０９ａをパケット解読手段３０１に対して出力し、１３９４バス１０５から受信したエイシンクロナスパケットの鍵情報２０３ａを鍵入手手段３０２に対して出力する手段である。また、Ｄ－ＩＦ１３９４入出力手段１０２ａは、鍵入手手段３０２の出力する、エイシンクロナスパケットである鍵情報転送要求を１３９４バス１０５に対して出力する手段である。

【００４６】パケット解読手段３０１は、Ｄ－ＩＦ１３９４入出力手段１０２ａからのデータパケット２０９ａを得て、パケットの内、Ｓｙフィールド９１０（図６参照）から２ビットのデータを抽出し、その２ビットデータの内容を解読して、抽出した２ビットデータをモード検出手段３０３へ送り、又、それがインートランジションモード（変更情報）を示している場合には、抽出した２ビットデータを復号化手段３０４へも送る手段である。又、パケット解読手段３０１は、２ビットデータの内容を解読した結果に応じて、パケットの内の実データ９０５（図６参照）を復号化手段３０４、又はデータ記録再生手段３０５へ送る手段である。

【００４７】モード検出手段３０３は、パケット解読手段３０１から送られてきたコピー管理情報の内容を調べ、調べた結果に応じて、実データ９０５の復号用の鍵を入手する必要がある旨の情報を鍵入手手段３０２へ送る手段である。

【００４８】鍵入手手段３０２は、モード検出手段３０３から上記情報が送られてきた場合、鍵の入手を開始するための鍵情報の転送要求をＤ－ＩＦ１３９４入出力手段１０２ａに送る手段である。尚、ここで重要なことは、この転送要求には、モード検出手段３０３から送られてきたコピー管理情報が添付されていることである。

【００４９】尚、このコピー管理情報の添付は，コピー管理情報をそのまま添付しても良いし，何らかの値に変換してから添付しても良い。所定の変換して添付する場合には，送信装置１０１は変換のルールを知っており，変換前のコピー管理情報を検出することが出来る。所定の変換の例としては、例えば、２ビットの０１を４ビットの０１００に変換し、１０を００１０に変換するという変換をして、この４ビットを送る構成が考えられる。

【００５０】又、鍵入手手段３０２は、送信装置１０１側から転送されてきた鍵情報２０３ａを鍵保存手段３０６へ送る手段である。尚、本発明のデータ管理情報検出手段は、パケット解読手段３０１と、モード検出手段３０３を含むものである。

【００５１】鍵保存手段３０６は、鍵入手手段３０２から送られてきた鍵情報を一時的に保存し、所定のタイミ

ングで復号化手段３０４へその鍵情報を出力する手段である。

【００５２】復号化手段３０４は、鍵保存手段３０６からの鍵情報とパケット解読手段３０１からの鍵の変更情報３１０とを利用して、実データ９０５を復号化する手段である。

【００５３】データ記録再生手段３０５は、復号化手段３０４で復号化されたＡＶデータを又は、パケット解読手段３０１から直接送られてきたＡＶデータを表示手段３０７へ送り表示させる手段であり、内蔵する記録媒体に記録する手段である。又、音声出力手段３０８は、データ記録再生手段３０５からの音声データを出力する手段である。

【００５４】尚、その他の受信装置１０３～１０４についても、上記と同様の構成である。

【００５５】以上の構成において、次に、本実施の形態の動作を図２～図４を参照しながら述べながら、本発明のデータ送信方法、データ受信方法の一実施の形態についても同時に説明する。

【００５６】図４は、本実施の形態のＳｙフィールド９１０（図６参照）に格納された２ビットデータ及び暗号鍵の時間的変化を示す図である。

【００５７】図４に示すように、本実施の形態では、送信装置１０１は、時刻Ｔ１までは第１のＡＶデータ４０１を、時刻Ｔ１からＴ６の間では第２のＡＶデータ４０２を、そして、時刻Ｔ６からＴ７の間では音声データ４０３を、更に、その後は、第３のＡＶデータ４０４を１３９４バス１０５上に転送しているものとする。

【００５８】又、これら転送データのコピー管理情報は、同図に示すとおり、それぞれ、前から順番に、コピー禁止、コピー１回可能、コピーフリー、そしてコピー禁止である。従って、各転送データと、使用する鍵のグループとの対応関係は、同図に示すとおり、第１のＡＶデータ４０１、第２のＡＶデータ４０２、そして第３のＡＶデータ４０４の転送は、それぞれこの順番にグループＢ、グループＡ、そしてグループＢがそれぞれ対応する。又、音声データ４０３は、コピーフリーであり、暗号化されないので該当するグループは存在しない。更に又、第２のＡＶデータ４０２の転送中に、グループＡの中で暗号鍵が３回更新（鍵Ａ１～Ａ３）されるものとする。

【００５９】（１）先ず、時刻Ｔ１直後における動作を述べる。

【００６０】即ち、モード決定手段２０２（図２参照）は、データ出力手段２０１から出力されてくる第２のＡＶデータのコピー管理情報を検出して、コピー１回可能であること判定し、それに対応する暗号鍵のグループをＡと決めて、鍵発生手段２０３に伝える。鍵発生手段２０３は、グループＡにおいて、暗号鍵Ａ１を作成して、鍵保存手段２０４へ送る。暗号化手段２０５は、鍵保存手段２０４から送られてきた暗号鍵Ａ１を用いて、第２のＡＶデータ４０２を暗号化する。パケット生成手段２０９は、暗号化された第２のＡＶデータ４０２を実データ９０５とし、変更情報発生手段２０８を介して送られてきたコピー管理情報の「１０」をＳｙフィールド９１０に格納して、データパケットとしてＤ－ＩＦ１３９４入出力手段１０１ａに出力する。

【００６１】一方、受信装置１０２（図３参照）では、１３９４バス１０５上に転送された第２のＡＶデータ４０２を含むデータパケットをＤ－ＩＦ１３９４入出力手段１０２ａを介して受信する。

【００６２】具体的には、パケット解読手段３０１が、受信されたデータパケットからＳｙフィールド９１０に格納さているコピー管理情報である２ビットデータ「１０」を抽出し、その内容から実データ９０５が暗号化されていること判定する。そして、実データ９０５の復号用の鍵を入手する必要がある旨の情報として、上記２ビットデータ「１０」を鍵入手手段３０２へ送る。鍵入手手段３０２は、２ビットデータ「１０」と送信装置の識別番号とを添えて、暗号鍵の入手を開始するための鍵情報の転送要求をＤ－ＩＦ１３９４入出力手段１０２ａに送る。尚、送信装置の識別番号は、ソースＩＤ９０６（図６参照）に格納されているものである。

【００６３】尚、転送要求へのコピー管理情報の添付のやり方には、上述した通り、２通りのやり方がある。これに関しては、以下に述べる場合においても同様である。

【００６４】送信装置１０１（図２参照）では、受信装置１０２からの鍵情報の転送要求を受信する。鍵配布手段２０６は、上記転送要求の発信元との所定の認証手続きを経た後、鍵発生手段２０３に対して、転送要求に付されている上記２ビットデータ「１０」（コピー管理情報）を送る。この認証手続きとは，相手が正しい機器であるかどうかを判定する為の手続きである．鍵発生手段２０３は、その「１０」に対応する暗号モード（即ち、鍵のグループ）及び、そのグループ内の対応する鍵がどれであるかを調べ、それが鍵のグループＡ内の鍵Ａ１であると判断した後、その鍵を生成するか、あるいは既に作成して保存されている同じ鍵Ａ１を得るかして、上記転送要求の発信元に対して転送する。尚、この様に、鍵配布手段２０６が、鍵保存手段２０４に保存されている暗号鍵Ａ１をそのまま転送せずに、わざわざ、転送要求に付されている上記２ビットデータ「１０」（コピー管理情報）を用いて、それに対応する鍵のグループ及び、そのグループ内の暗号鍵を調べることとしたのは、従来の課題の欄で述べた不正行為を防止するためである。これについては、更に後述する。

【００６５】一方、受信装置１０２（図３参照）では、鍵入手手段３０２が、送信装置１０１側から転送されてきた暗号鍵Ａ１を得て、鍵保存手段３０６へ送る。復号

化手段３０４は鍵保存手段３０６から得た、暗号鍵Ａ１を用いて、パケット解読手段３０１からの送られてきた暗号化されたデータを復号し、データ記録再生手段３０５に送る。

【００６６】データ記録再生手段３０５は、Ｓｙフィールド９１０に格納されているデータ「１０」がコピー１回可能であることを判定して、内蔵する記録媒体に、復号化された第２のＡＶデータを記録しながら、表示手段３０７、音声出力手段３０８にも同時に出力する。

【００６７】ここで、データ記録再生手段３０５は、第２のＡＶデータを記録する場合、Ｓｙフィールド９１０に格納されているコピー管理情報である「１０」のデータを「１１」と書き換えた上で上記記録動作を行うものである。これは、上記記録によりコピーが１回実行されたことになり、その記録媒体からのその後のコピーは禁止すべきだからである。但し、実データ９０５の中に含まれているコピー管理情報の書き換えは行わない。尚、第２のＡＶデータの転送が開始されるＴ１時刻においては、暗号鍵がその直前に使用していたものとは変化しているので、受信装置１０２は、上述の様に新たな鍵を入手するまでは、第２のＡＶデータを復号出来ないという問題を避けるため、第２のＡＶデータの送信開始からしばらくの間は、暗号化を行わないようにしても勿論良い。ここで、しばらくの間とは、例えば、受信装置１０２側において、新たな鍵の入手が完了するまでの間である。

【００６８】（２）次に、時刻Ｔ２～Ｔ３における動作を述べる。

【００６９】この間は、Ｓｙフィールド９１０にインートランジションモードを示す変更情報「０１」が格納されている。受信装置１０２のパケット解読手段３０１は、Ｓｙフィールド９１０に２ビットデータ「０１」が格納されていることを検出すると、その変更情報「０１」を復号化手段３０４へ送り、鍵の更新がある旨を予告し、復号化手段３０４は、新たな復号処理の準備を開始する。又、モード検出手段３０３は、上記２ビットデータ「０１」が変更情報であることを検出して、鍵入手手段３０２に対して、新たな鍵の入手が必要である旨を伝える。ここでも、所定時間後に変更される予定の新たな鍵の転送要求に際し、上述した通り、コピー管理情報が必要となる。しかし、この場合、Ｓｙフィールド９１０には、コピー管理情報は格納されていないので、インートランジションモードの情報が送られてくる直前前に送られてきたコピー管理情報の「１０」を使用する。従って、鍵入手手段３０２は、送信装置１０１に対して、直前のコピー管理情報の「１０」を添えて上記鍵の転送要求を出す。

【００７０】尚、鍵のグループが変更されていないので、コピー管理情報の「１０」を送らない構成としてもかまわない。

【００７１】一方、送信装置１０１では、鍵配布手段２０６が上記新たな鍵の転送要求を受けて、切り替えタイミング決定手段２０７により決定される時刻Ｔ３から使用される予定の新たな鍵Ａ２の生成を鍵発生手段２０３へ要求し、生成された新たな鍵Ａ２を受信装置１０２側へ転送する。時刻Ｔ１においては，受信装置１０２からの鍵情報の転送要求を受信した送信装置１０１は、鍵を転送要求の発信元に対して転送する前に上記転送要求の発信元との所定の認証手続きを行っていた．この様に既に認証手続きが終了しているので，今回は（即ち、時刻Ｔ２から時刻Ｔ３の間では）、鍵の転送前に再度認証手続きを行う必要はない．尚、生成された鍵Ａ２は、鍵保存手段２０４へも送られる。又、鍵配布手段２０６は、所定のやりとりの結果、受信装置１０２への鍵の配布が完了したことを確認して、配布完了情報２０６ａを切り替えタイミング決定手段２０７へ送る。切り替えタイミング決定手段２０７は、配布完了情報を得た後、暗号化手段２０５に対して、それまで使用していた鍵を鍵保存手段２０４から得た新たな鍵Ａ２に変更して、暗号化を行うことを指示する。これにより、時刻Ｔ３からは、暗号鍵Ａ'2により暗号化された第２のＡＶデータ４０２がデータパケットとして１３９４バス１０５上に転送される。

【００７２】受信装置１０２側では、既に新たな鍵Ａ２は入手完了しているので、暗号鍵Ａ２により暗号化された第２のＡＶデータ４０２がデータパケットととして受信した場合でも、問題なく復号出来る。その後の動作は、上述した（１）の場合と同様である。

【００７３】（３）次に、時刻Ｔ４～Ｔ５における動作を述べる。

【００７４】この場合は、新たな鍵が鍵Ａ３である点を除いて、上記（２）と同様である。

【００７５】尚、このように、同一のモード内においても、暗号鍵を時間とともに更新することとしたのは、暗号化の安全性をより一層確保するためである。即ち、同じ鍵の使用時間が長くなるほど、不正行為による暗号の解読のチャンスが増加する。

【００７６】一方、同一鍵による暗号化データの蓄積量も大きくなり、仮に、暗号が不正に解読された場合の被害も大きくなることを考慮したものである。

【００７７】（４）次に、時刻Ｔ６における動作を述べる。

【００７８】この場合は、時刻Ｔ６においてコピーフリーの音声データ４０３の転送が開始されるので、暗号鍵は存在しない。従って、時刻Ｔ６の直前では、上述の様な予告としての変更情報「０１」は出されない。

【００７９】受信装置１０２では、パケット解読手段３０１が、受信されたデータパケットのＳｙフィールド９１０に「００」が格納されていることを検出して、実データ９０５は暗号化されていないと判定して、実データ

９０５をデータ記録再生手段３０５へ直接送る。又、送信装置１０１に対する鍵の転送要求も行わない。データ記録再生手段３０５での動作は、上述した内容と同様である。

【００８０】（５）次に、時刻Ｔ７における動作を述べる。

【００８１】この場合、転送対象のデータが第３のＡＶデータ４０４であり、これがコピー禁止のデータであることから、上記（１）の場合と動作内容は同じである。尚、本実施の形態では、上述した不正な暗号の解読を防止するという主旨から、同一のコピー管理情報が与えられている転送データにおいて、それぞれが別個独立のものであるか、あるいは、それぞれが時間的に不連続であるかに関わらず、時間とともに暗号鍵を更新するものであり、ここでも、第１のＡＶデータ４０１の暗号化に使用した鍵Ｂ１から鍵Ｂ２に変更している。但し、鍵Ｂ１も鍵Ｂ２も、鍵のグループは同じグループＢに属している。

【００８２】ところで、第３のＡＶデータを受信する場合を例にとり、上述した通り、コピー管理情報を改竄したとしてもそれ以上の不正行為を防止することが出来る点について詳細に述べる。

【００８３】即ち、１３９４バス１０５上のどこかで不正行為が行われ、受信装置１０２が受信した第３のＡＶデータ４０４において、Ｓｙフィールドの「１１」情報が「１０」に改竄されている場合を考える。

【００８４】鍵入手手段３０２（図３参照）は、上述したとおり、この改竄された「１０」のデータを添えて、上記鍵の転送要求を行う。この転送要求を得た、鍵配布手段２０６（図２参照）は、添えられている「１０」を鍵発生手段２０３へ送り、鍵発生手段２０３は、「１０」に対応する鍵のグループ及び、そのグループ内の暗号鍵を調べ、グループＡに属する鍵であると判断して、グループＡに属する鍵を生成し、それが受信装置１０２へ送られる。受信装置１０２の復号化手段３０４は、第３のＡＶデータ４０４の復号に、グループＡに属する鍵を使用しても正しい復号は行えない。本来の鍵は、グループＢに属する鍵Ｂ２であるからである。

【００８５】従って、データ記録再生手段３０５は、正しく復号されない意味不明の状態のデータをコピー管理情報「１０」の内容通り、１回だけ記録媒体に記録するが、このような記録データは全く使用価値が無く、不正行為は無駄な行為となるのである。又、この場合、表示手段３０７への表示も意味不明の画像となる。尚、正しく復号されなかったデータについては、記録動作を行わない様にデータ記録再生手段３０５を構成しておいても勿論良い。

【００８６】尚、本発明の暗号化の種類は、上記実施の形態では、暗号鍵であったが、これに限らず例えば、暗号のアルゴリズムであっても良い。この場合、送信対象となるデータの管理情報に応じて上記データの送信に適用する暗号のアルゴリズムを変える構成となる。又、そのアルゴリズムの変え方として具体的には、例えば、大きく分けて次の様な２通りのやり方がある。即ち、一つは、暗号化処理手順の順番を入れ替えることにより、暗号のアルゴリズムを異ならせるものであり、他の一つは、暗号化処理手順のループ回数を変えることにより、暗号のアルゴリズムを異ならせるものである。前者の場合、例えば、所定データに対して、第１の暗号化処理を適用し、その処理結果に対して、更に、第２の暗号化処理を適用した場合の暗号化データと、上記第１と第２の暗号化処理の順番を逆に適用した場合の暗号化データとが異なるという特性を利用するものであり、暗号化回路等のハードウェアーの構成を複雑にすることなく実現出来るものである。尚、この場合、双方の暗号化データの暗号の強度は同じレベルである。又、後者の場合、例えば、所定データに対して、第１の暗号化処理を適用し、その結果に対して、更に同じ暗号化処理を適用するという動作の繰り返し回数を一般にループ回数というが、このループ回数を変えることにより、暗号化データを異ならせるというものである。尚、この場合、一般にループ回数を多くしたものほど暗号の強度が上がる。又、言うまでもなく、前者と後者を組み合わせてたものとして、暗号化処理手順の順番を変え、且つ、各暗号化処理のループ回数も変える構成でも良い。更に又、上記の場合、暗号鍵は同一でも良いし、異ならせても良い。以上述べた、暗号のアルゴリズムを変えるという構成を適用する場合、送信装置が、受信装置側に対して送信すべき復号化情報としては、前者の場合は、例えば、暗号化処理の順番であり、後者の場合は、例えば、ループ回数である。

【００８７】又、上記実施の形態では、データ記録再生手段が、コピー１回可能とされるデータの記録の際に、Ｓｙフィールドに格納されているコピー管理情報を書き換えることについて説明した。ここでは、その点について更に述べる。上記実施の形態でも述べた様に、データ記録再生手段は、実データの中に含まれているコピー管理情報までは書き換えない。そのため、その記録データが、その後、別の記録装置等に送信される場合、Ｓｙフィールド内の情報と、実データ内の情報が一致していないため、その別の記録装置において混乱が生じることも考えられる。そこで、本来は、双方の情報は一致させるべきものであるが、装置の構成が複雑になることを避けるため、あえて不一致状態を許し、その代わり、Ｓｙフィールドには、その旨を示す情報を書き込む構成としても良い。即ち、コピー１回可能のデータを受信し記録した後、送信する際に、実データ内のコピー管理情報は書き換えていないが、実データのコピーは禁止であることを示す情報として、新たに「ストリームコピー」と名付け、Ｓｙフィールドに格納する２ビットデータは「０

１」とするものである。この場合、データ記録再生手段３０５は、ＡＶデータを記録する場合、Ｓｙフィールド９１０に格納されているコピー管理情報である「１０」のデータを、更なるコピー禁止を意味する「０１」と書き換えた上で上記記録動作を行う。これにより、正規の装置においては、コピー管理情報としてもともとコピー禁止であるというデータと、１回コピーが実行されたために、その後のコピーが禁止であるというデータの区別が可能となる。従って、Ｓｙフィールド内の情報により、混乱無く正しく動作させることが可能となる。更に又、この場合、上記実施の形態で述べたものと同様の構成により、コピー管理情報としての「ストリームコピー」に対応した新たな暗号化の種類（例えば、暗号鍵のグループＣ）を設けることが出来る。つまり、上述の様に、コピー１回可能のデータが受信され記録された後、その記録データ（第２世代のデータ）を更に送信する装置があった場合、その第２世代のデータのコピー管理情報についても、上記と同様の効果を発揮出来る様にするためである。

【００８８】又、この場合、上記実施の形態で述べた、インートランジション情報は、Ｓｙフィールドでは、表せないので、例えば、アイソクロノスパケットヘッダ９００内の、Ｓｙフィールド９１０とは別の領域に独立した１ビットとして確保し、そこに格納する構成としても良い。

【００８９】又、上記実施の形態では、インートランジション情報「０１」がＳＹフィールド９１０に格納される場合について述べたが、これに限らず例えば、アイソクロノスパケットヘッダ９００内の、Ｓｙフィールド９１０とは別の領域に独立した１ビットを確保し、そこに格納する構成としても良い。

【００９０】又、上記実施の形態では、受信装置が、時間とともに変化する鍵の予告情報を受けた後、新たな鍵の転送要求を出す場合について述べた。しかし、これに限らず例えば、送信装置は、上記予告情報の代わりに更新情報を送信し、その更新情報を受信した受信装置から鍵の転送要求が有った場合、上記送信装置が、その転送を要求された鍵に加えて、次に使用する予定の鍵も同時に送るという構成でも良い。ここで、上記更新情報は、鍵の種類（即ち、暗号化の種類）が、上述の様に時間と共に更新される場合に、その更新が実行されたことを受信装置に通知するための情報であり、変更情報発生手段２０８により生成される（図２参照）。尚、本発明の更新実行情報生成手段は、この変更情報発生手段２０８に対応する。

【００９１】この場合、図５に示すように、独立した１ビットを確保したインートランジション情報が、上記更新情報に対応するものであり、新たな鍵を使用するタイミングを受信装置に知らせることになる。

【００９２】即ち、図５において、受信装置は、時刻Ｔ１の直後に鍵Ａ１と鍵Ａ２とを同時に入手しており、時刻Ｔ３の時点で、インートランジション情報が、０から１に反転すると、この反転のタイミングを検出した受信装置は、新たな鍵（鍵Ａ２）の使用を開始する。又、この時、受信装置は送信装置に対し、上述した通り、鍵の転送要求を行う。この転送要求に対して、送信装置から現在使用中の鍵Ａ２と、次に使用する予定の鍵Ａ３とが同時に送られてくる。従って、鍵Ａ２については、既に送ったものと重複することになる。そこで、受信装置は、鍵Ａ３についてはこれを保持するが、鍵Ａ２については、既に取得した鍵をそのまま使用し、２度目に送られてきた鍵Ａ２は捨てる。尚、これとは異なり、既に取得した鍵を、２度目に送られてきた鍵Ａ２と差し替えて使用しても勿論良い。

【００９３】又、図５において、時刻Ｔ５では、１から０に反転するので、この反転を検出した後は、上記と同様の動作となる。上記内容は、勿論、暗号鍵に限らず、例えば、暗号のアルゴリズムを変える場合でも同様に適用出来る。

【００９４】また，上記各実施実施の形態では，説明を簡単にするために復号化情報として鍵をそのまま送信していたが，復号化情報はこれに限るものではなく，受信装置が鍵を作成できる情報であればどのような情報であってもよい．例えば，鍵を暗号化して受信装置に送信し，受信装置は暗号化された鍵を復号化して鍵自身を入手するようにしてもよい．この復号化に必要な情報は認証手続きの際に送信装置と受信装置との間で共有したり，装置製造時に予め送信装置と受信装置に記憶させておいても良い．このようにすれば、鍵の送信を第３者に盗聴されたとしても、第３者には鍵が渡らない。

【００９５】又、上記実施の形態では、同一のコピー管理情報のデータについても、暗号化鍵を時間とともに異ならせる場合について述べたが、これに限らず例えば、コピー管理情報に応じて、鍵や暗号化のアルゴリズムを異ならせる構成であれば、時間的に異ならせなくてもかまわない。

【００９６】又、上記実施の形態では、コピー管理情報として、コピーフリー、コピー１回可能、コピー禁止などを用いる場合について述べたが、これに限らず例えば、コピー回数の異なるものがあっても勿論良く、これらに限るものではない。

【００９７】又、以上述べた実施の形態及びそれらの変形例の何れか一つの例に記載の各手段の全部又は一部の手段の機能をコンピュータに実行させるためのプログラムを記録した磁気記録媒体や光記録媒体などの記録媒体を作成し、それを利用することにより上記と同様の動作を実行させることが出来る。

【００９８】又、上記実施の形態及びそれらの変形例の各手段の処理動作は、コンピュータを用いてプログラムの働きにより、ソフトウェア的に実現してもよいし、あ

るいは、上記処理動作をコンピュータを使用せずに特有の回路構成により、ハードウェア的に実現してもよい。

【００９９】

【発明の効果】以上述べたところから明らかなように本発明は、伝送データの保護が従来に比べてより一層確実に行えるという長所を有する。

【図面の簡単な説明】

【図１】本発明の実施の形態におけるデータ伝送システムの概略構成図

【図２】同実施の形態における送信装置の構成を示すブロック図

【図３】同実施の形態における受信装置の構成を示すブロック図

【図４】同実施の形態における、暗号鍵の時刻による変化を示す説明図

【図５】本発明の別の実施の形態における、暗号鍵の時刻による変化を示す説明図

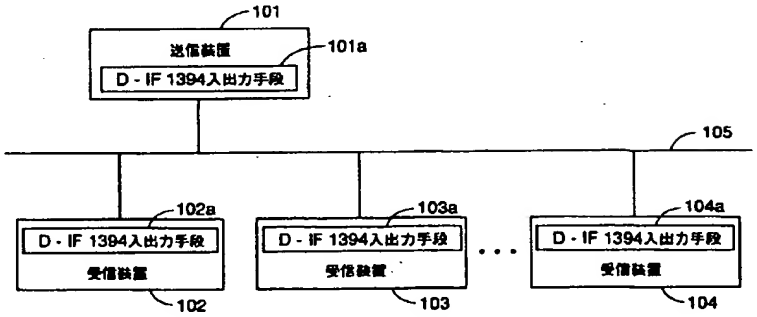
【図６】従来のデータ転送方法におけるアイソクロノスパケットのフォーマットを表す説明図

【符号の説明】

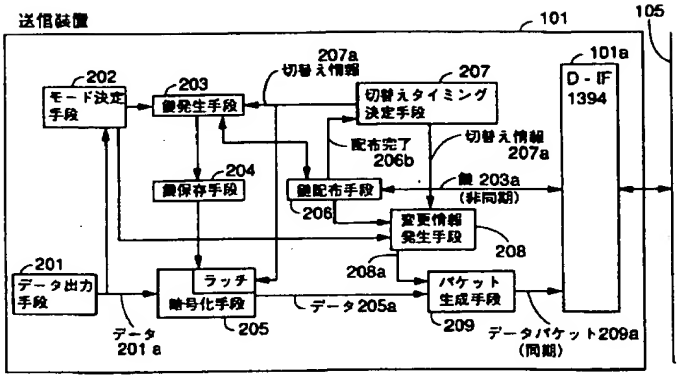
１０１　　送信装置

１０１ａ	１３９４入出力手段（データ送信手段）
１０２ａ	１３９４入出力手段（データ受信手段）
１０２～１０４	受信装置
１０５	ＩＥＥＥ１３９４バス
２０２	モード決定手段
２０３	鍵発生手段（暗号化種類更新手段）
２０６	鍵配布手段（復号化情報送信手段）
２０７	切り替えタイミング決定手段（暗号化種類更新手段）
２０８	変更情報発生手段（予告情報生成手段）
３０１	パケット解読手段（データ管理情報検出手段）
３０２	鍵入手手段（復号化情報要求手段）
３０３	モード検出手段
３０４	復号化手段
３０５	データ記録再生手段（処理方法決定手段）
４０１	第１のＡＶデータ

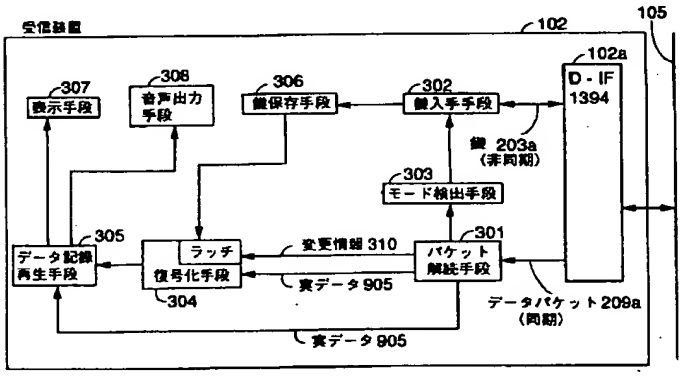
【図１】



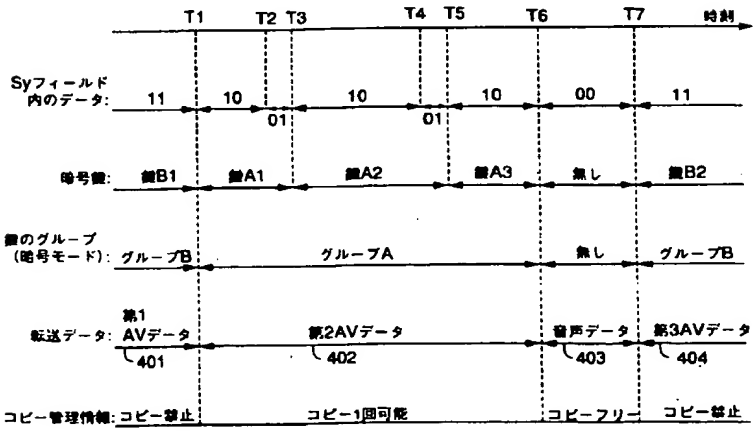
【図２】


送信装置
101
105
101a
D - IF
1394
202
モード決定
手段
203
鍵発生手段
207a
切替え情報
207
切替えタイミング
決定手段
配布完了
206b
切替え情報
207a
204
鍵保存手段
鍵配布手段
鍵 203a
(非同期)
206
変更情報
発生手段
208
208a
201
データ出力
手段
ラッチ
暗号化手段
データ205a
パケット
生成手段
データ
201 a
205
209
データパケット209a
(同期)

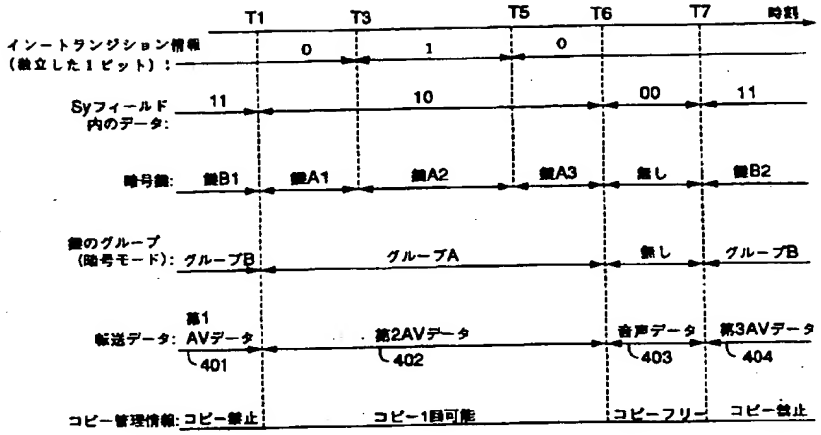
【図３】


受信装置
102
105
102a
D - IF
1394
307
表示手段
308
音声出力
手段
306
鍵保存手段
302
鍵入手段
鍵 203a
(非同期)
303
モード検出手段
305
データ記録
再生手段
ラッチ
復号化手段
変更情報 310
実データ 905
304
301
パケット
解読手段
データパケット209a
(同期)
実データ 905

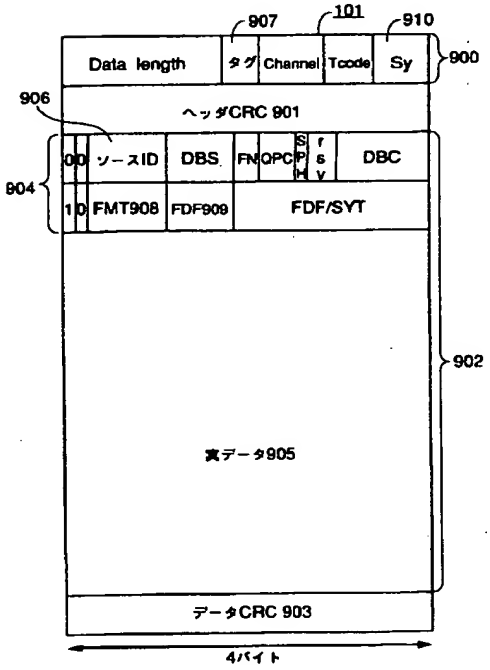
【図４】


T1
T2
T3
T4
T5
T6
T7
時刻
Syフィールド
内のデータ:
11
10
01
10
01
10
00
11
暗号鍵:
鍵B1
鍵A1
鍵A2
鍵A3
無し
鍵B2
鍵のグループ
(暗号モード):
グループB
グループA
無し
グループB
転送データ:
第1
AVデータ
401
第2AVデータ
402
音声データ
403
第3AVデータ
404
コピー管理情報:
コピー禁止
コピー1回可能
コピーフリー
コピー禁止

【図５】


T1
T3
T5
T6
T7
時刻
インートランジション情報
（立上した１ビット）：
0
1
0
Syフィールド
内のデータ:
11
10
00
11
暗号鍵:
鍵B1
鍵A1
鍵A2
鍵A3
無し
鍵B2
鍵のグループ
（暗号モード）:
グループB
グループA
無し
グループB
転送データ:
第1
AVデータ
401
第2AVデータ
402
音声データ
403
第3AVデータ
404
コピー管理情報:
コピー禁止
コピー1回可能
コピーフリー
コピー禁止

【図６】


907
101
910
Data length
タグ
Channel
Tcode
Sy
900
906
ヘッダCRC 901
00
ソースID
DBS
FN
QPC
SPH
rsv
DBC
904
10
FMT908
FDF909
FDF/SYT
902
実データ905
データCRC 903
4バイト

フロントページの続き

(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器
産業株式会社内